CAR2-701

User Manual

V1.1.1

Contents

1 Introduction 1
1.1 Safety Precautions 1
1.2 LEDs and Interfaces 2
1.3 System Requirements 3
1.4 Features 3
2 Hardware Installation 5
3 Web Configuration 8
3.1 Access the Router 8
3.2 Status 9
3.3 Wizard 11
3.4 Setup 14
3.4.1 WAN Configuration 14
3.4.2 LAN Configuration 21
3.5 Advanced 30
3.5.1 Route 30
3.5.2 NAT 34
3.5.3 QoS 41
3.5.4 CWMP 44
3.5.5 Others 46
3.6 Service 50
3.6.1 IGMP 50
3.6.2 UPnP 52
3.6.3 SNMP 53
3.6.4 DNS 54
3.6.5 DDNS 56
3.6.6 FTP Server 57
3.7 Firewall 57
3.7.1 MAC Filter 57
3.7.2 IP/Port Filter 58
3.7.3 URL Filter 60
3.7.4 ACL 61
3.7.5 DoS 66
3.8 Maintenance 67
3.8.1 Update 68

3.8.2 Password 69
3.8.3 Reboot 70
3.8.4 Time 71
3.8.5 Log 73
3.8.6 Diagnostics 73
4 Troubleshooting 81

1 Introduction

The CAR2-701 is 1-Port ADSL 2/2+ Modem Router and it is an ADSL access device that supports multiple line modes. It provides one 10/100Base-T Ethernet interface at the user end and provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. The device provides high performance access to the Internet.

1.1 Safety Precautions

Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

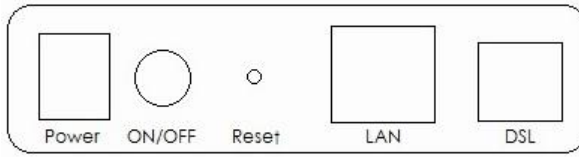
1.2 LEDs and Interfaces

- **Front Panel**

The following table describes the LEDs of the device:

LEDs	Status	Description
Power	On	The device is powered on
	Off	The device is powered off
LAN	On	There is a successful connection on the LAN port
	Off	There is no connection on the LAN port
	Blinking	Data is being transferred over the LAN port
DSL	On	DSL link up/link synchronized
	Blinking	Link training/DSL link not synchronized
Internet	On	Successful PPP session
	Off	Before DSL link up
	Blinking	There is data being transmitted or received

- **Rear Panel**



The following table describes the interfaces of the device:

Interface	Description
Power	Power interface for connecting to the power adapter.
ON/OFF	Power switch for powering on/ off the device.
Reset	Reset to the factory defaults. To reset to the factory defaults, you should keep the device powered on, push a needle into the hole and then press and hold more than 5 seconds.
LAN	RJ-45 interface for connecting to the Ethernet interface of PC or other Ethernet devices through the Ethernet cable.
DSL	RJ-11 interface for connecting to the ADSL interface or a splitter through the telephone cable.

1.3 System Requirements

Recommended system requirements are as follows.

- A 10/100 base-T Ethernet card installed in your PC
- A hub or Switch (connected to several PCs through the Ethernet interface on the device)
- Operating system: Windows 98 SE, Windows 2000, Windows ME, Windows XP，Windows 7 or higher
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.4 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483Briged/1483Routed/MER/IPoA access
- Multiple PVCs (up to eight) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- 802.1Q and 802.1P protocol

- DHCP server
- NAPT
- Static route
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- DNS
- Virtual server
- DMZ
- Two-level passwords and usernames
- Web interface
- Telnet CLI
- System status display
- PPP session PAP/CHAP
- IP filter
- IP quality of service (QoS)
- Remote access control
- Line connection status test
- Remote managing through Telnet or HTTP
- Backup and restoration of configuration file
- Ethernet interface supporting crossover detection, auto-correction, and polarity correction
- Universal plug and play (UPnP)

2 Hardware Installation

Step 1 Connect the **DSL** interface of the device and the **Modem** interface of the splitter through a telephone cable. Connect the phone to the **Phone** interface of the splitter through a cable. Connect the incoming line to the **Line** interface of the splitter.

The splitter has three interfaces:

- **Line**: Connect to a wall phone jack (RJ-11 jack).
- **Modem**: Connect to the ADSL jack of the device.
- **Phone**: Connect to a telephone set.

Step 2 Connect the **LAN** interface of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:
Use twisted-pair cables to connect with the hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** interface of the device.

Connection 1

Figure1 shows the application diagram for the connection of the modem, PC, splitter, and telephone sets, when no telephone set is placed before the splitter. This type of connection is recommended.

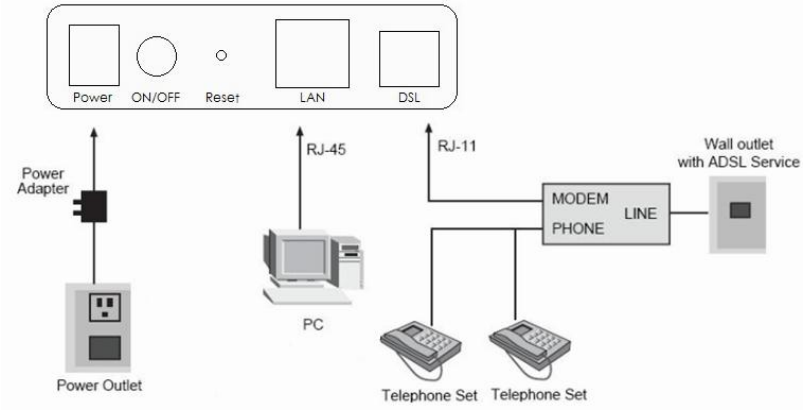


Figure1 Connection diagram (Without connecting telephone sets before the splitter)

Connection 2

0 shows the connection when the splitter is installed close to the router.

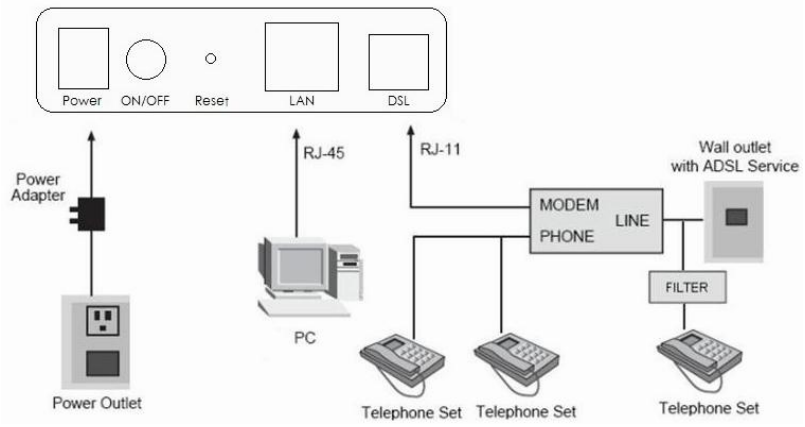


Figure2 Connection diagram (A telephone set is placed before the splitter)

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure2. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

3 Web Configuration

This chapter describes how to configure the router by using the Web-based configuration utility.

3.1 Access the Router

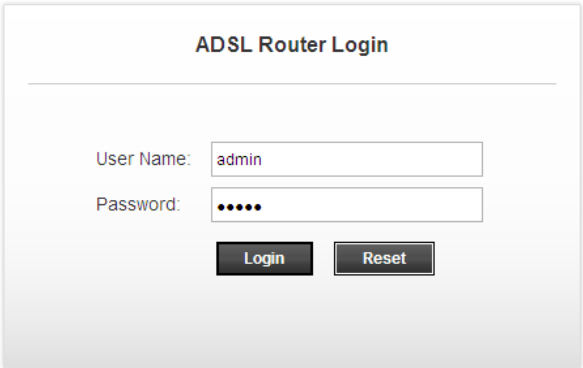
The following is the detailed description of accessing the router for the first time.

Configure the IP address of the PC as 192.168.1.X (2~254), Subnet Mask as 255.255.255.0.

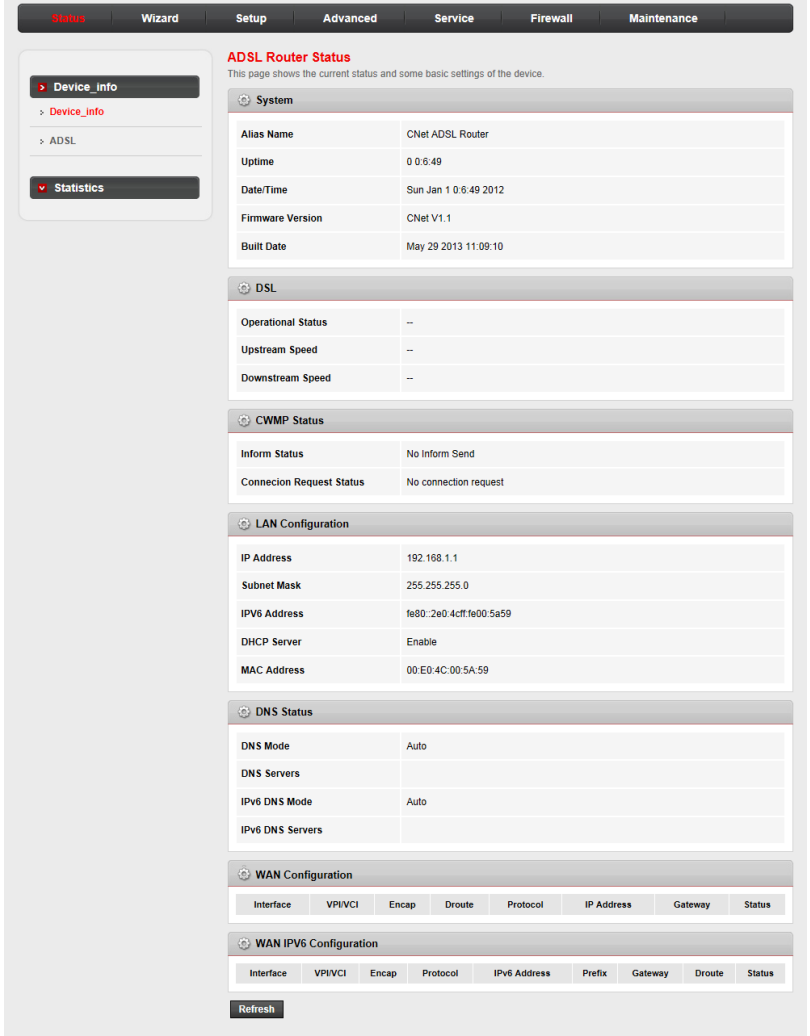
Step1 Open the Internet Explorer (IE) browser and enter **http://192.168.1.1**.

Step2 In the **Login** page that is displayed, enter the username and password, and then click **Login**.

- The username and password of the super user are **admin** and **admin**
- The username and password of the common user are **user** and **user**

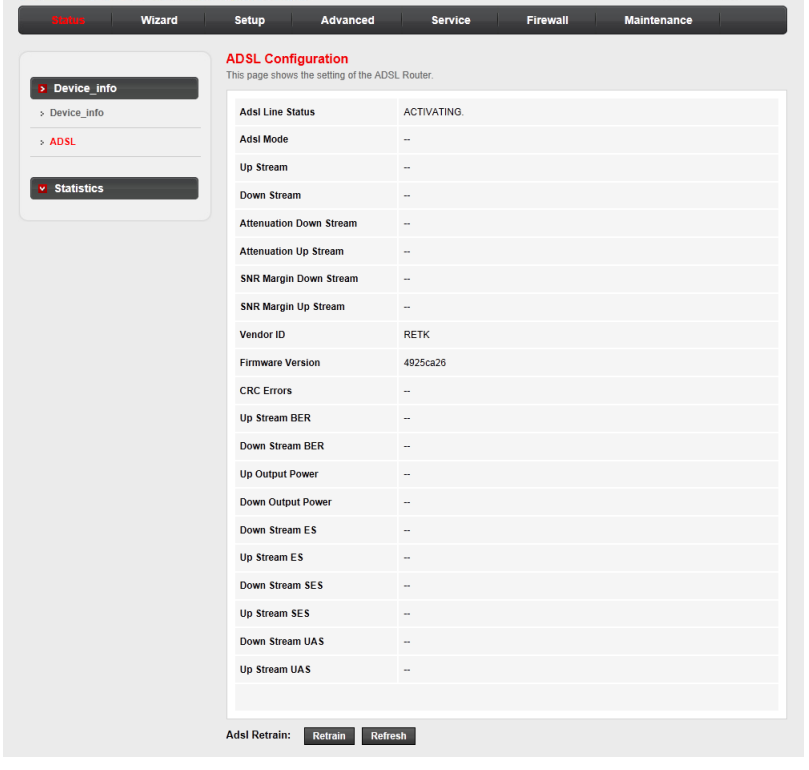


If you log in as a super user, you will see the **Device Info** page shown as below. You can check the basic settings of the modem, such as firmware version, upstream speed, downstream speed, LAN MAC address, LAN IP address, DHCP server status. You can also view the basic status of WAN and DNS Server.


Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Device_info
Device_info
ADSL
Statistics
ADSL Router Status
This page shows the current status and some basic settings of the device.
System
Alias Name
CNet ADSL Router
Uptime
0 0:6:49
Date/Time
Sun Jan 1 0:6:49 2012
Firmware Version
CNet V1.1
Built Date
May 29 2013 11:09:10
DSL
Operational Status
--
Upstream Speed
--
Downstream Speed
--
CWMP Status
Inform Status
No Inform Send
Connecion Request Status
No connection request
LAN Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
IPV6 Address
fe80::2e0:4cff:fe00:5a59
DHCP Server
Enable
MAC Address
00:E0:4C:00:5A:59
DNS Status
DNS Mode
Auto
DNS Servers
IPv6 DNS Mode
Auto
IPv6 DNS Servers
WAN Configuration
Interface
VPI/VCI
Encap
Droute
Protocol
IP Address
Gateway
Status
WAN IPV6 Configuration
Interface
VPI/VCI
Encap
Protocol
IPv6 Address
Prefix
Gateway
Droute
Status
Refresh

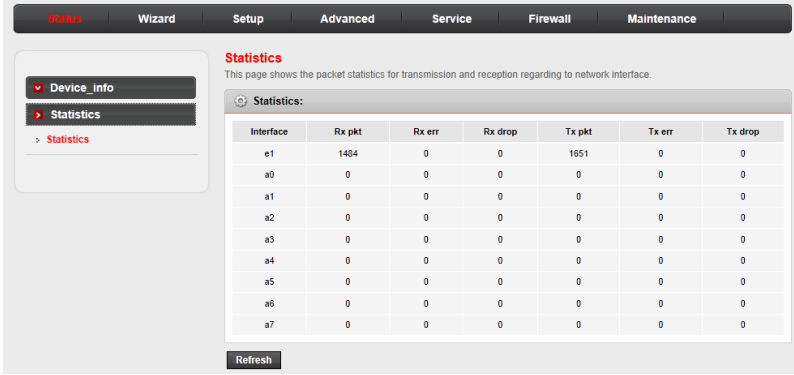
3.2 Status

The tab **Status** contains **Device Info** and **Statistics**. Choose **Status** > **Device Info** > **ADSL**, and the page is shown as the following figure. You can see the router settings such as the Adsl Line Status.



Click **Retrain**, the device interacts with the office end to reacquire the values and parameters of the router settings. If you want to refresh the page, click **Reflesh**.

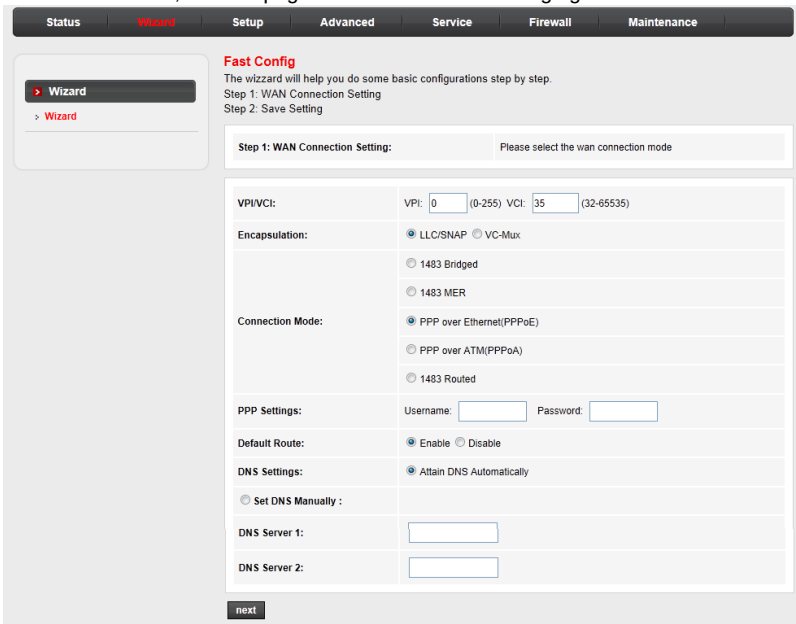
Choose **Status** > **Statistics**, and the page is shown as the following figure. In this page you can view the packet statistics for transmission and reception regarding to network interface.


Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Device_info
Statistics
Statistics
Statistics
This page shows the packet statistics for transmission and reception regarding to network interface.
Statistics:
Interface | Rx pkt | Rx err | Rx drop | Tx pkt | Tx err | Tx drop
e1 | 1484 | 0 | 0 | 1651 | 0 | 0
a0 | 0 | 0 | 0 | 0 | 0 | 0
a1 | 0 | 0 | 0 | 0 | 0 | 0
a2 | 0 | 0 | 0 | 0 | 0 | 0
a3 | 0 | 0 | 0 | 0 | 0 | 0
a4 | 0 | 0 | 0 | 0 | 0 | 0
a5 | 0 | 0 | 0 | 0 | 0 | 0
a6 | 0 | 0 | 0 | 0 | 0 | 0
a7 | 0 | 0 | 0 | 0 | 0 | 0
Refresh

Click Refresh to refresh this page.

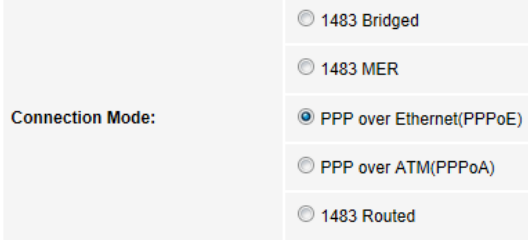
3.3 Wizard

Choose **Wizard**, and the page is shown as the following figure.

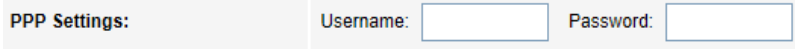


1) Change the VPI or VCI values which are used to define a unique path for your connection. If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP.

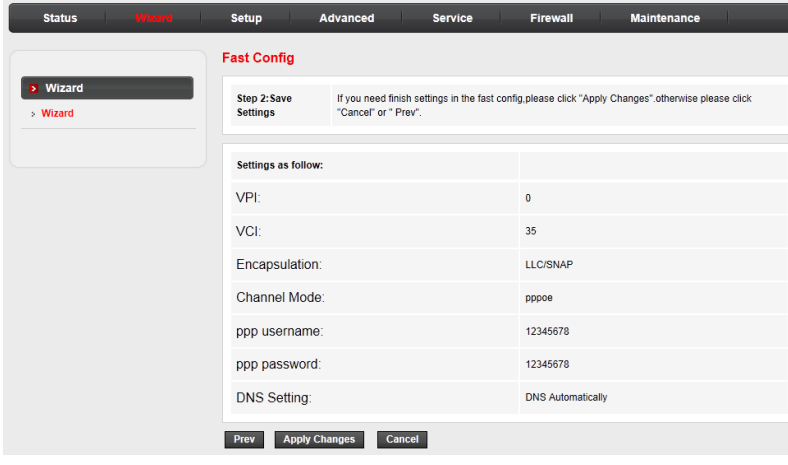
2) Please select the Connection Type given by your ISP.



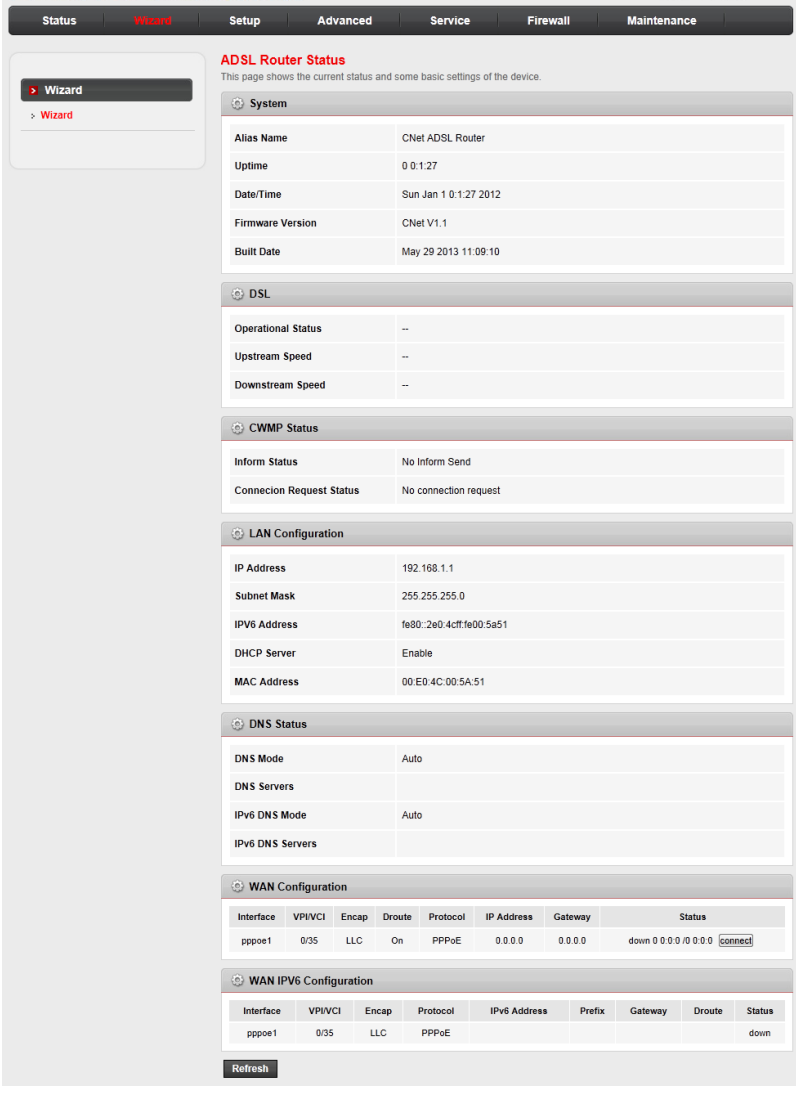
3) Here we use PPPoE as an example. Enter the Username, Password and Confirm Password given by your ISP, and then click Next.



4) On this page, please confirm all parameters. Click **Prev** to modify or click the **Apply Changes** button to save your configuration.



5) You will see the complete screen below:



3.4 Setup

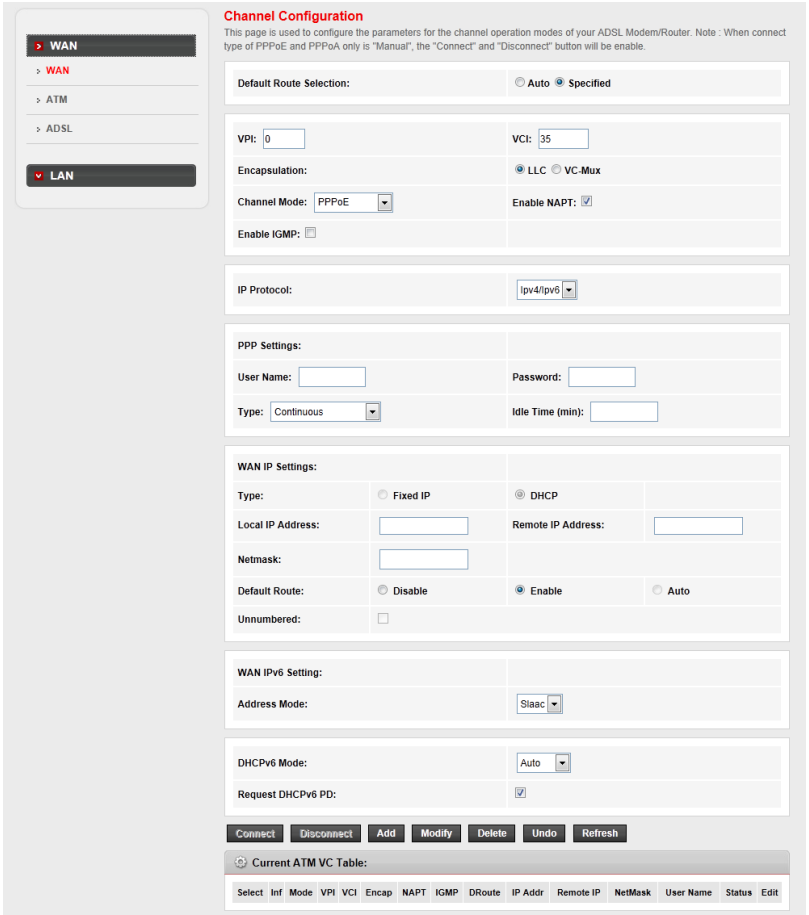
In the navigation bar, click **Setup**. The **Setup** contains **WAN** and **LAN** configuration.

3.4.1 WAN Configuration

In the **Setup** page, click **WAN** on the left pane, and the sub-menu of the **WAN** includes **WAN**, **ATM** and **ADSL**.

3.4.1.1 WAN

Choose **Setup** > **WAN,** and the page is shown as the following figure. In this page, you can configure WAN interface of your router.



The following table describes the parameters in this page:

Field	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by

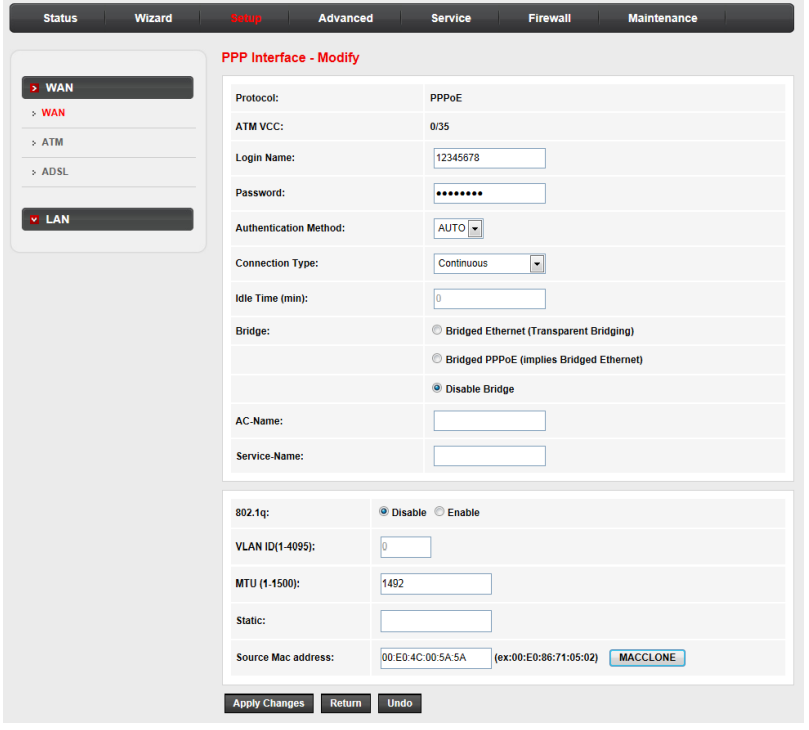
Field	Description
	your ISP.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. Enter the correct VCI provided by your ISP.
Encapsulation	You can select **LLC** or **VC-Mux**. In this example, the encapsulation mode is set to **LLC**.
Channel Mode	You can choose **1483 Bridged, 1483 MER, PPP over Ethernet (PPPoE)**, **PPP over ATM (PPPoA)**, **1483 Routed**, or **IPoA**.
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
IP Protocol	You can choose **IPv4/IPv6**, **IPv4** and **IPv6**.
PPP Settings (Note: the parameters of **PPP Settings** are only available in the mode of **PPPoE** and **PPPoA**.)	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand** or **Manual**.
Idle Time (min)	If set the type to **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings (Note: **WAN IP Settings** is only available in the mode of 1**483MER**, **1483 ROUTED** and **IPOA**.)	
Type	You can choose **Fixed IP** or **DHCP**. ● If select **Fixed IP**, you should enter the local IP

Field	Description
	address, remote IP address and subnet mask. ● If select **DHCP**, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the gateway IP address provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Default Route Selection	You can select **Auto** or **Specified**.
Unnumbered	Select this checkbox to enable IP unnumbered function.
WAN IPv6 Setting	Set IPv6 WAN setting if this interface supports IPv6
Address Mode	You can choose **Slaac** or **Static**. **Slaac**:IPv6 Stateless address autoconfiguration **Static**:IPv6 static address configuration
Enable DHCPv6 Client	Enable or disable DHCPv6 Client on this interface, if enable, user can specify if the DHCPv6 Client request Address or request Prefix.
Request Options	You can choose **Request Address** or **Request Prefix**.
Add	After configuring the parameters of this page, click it to add a new PVC into the **Current ATM VC Table**.
Modify	Select a PVC in the **Current ATM VC Table**, then modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
Delete	Select a PVC in the Current ATM VC Table, and then click **Delete** to delete it
Current ATM VC Table	This table shows the existed PVCs. It shows the interface name, channel mode, VPI/VCI, encapsulation mode, local IP address, remote IP address and other information. The maximum item of this table is eight.

After proper settings, click **Add** and the page is shown as the following figure.

Current ATM VC Table:
Select Inf Mode VPI VCI Encap NAPT IGMP DRoute IP Addr Remote IP NetMask User Name Status Edit
pppoe1 PPPoE 0 35 LLC On Off On 0.0.0.0 0.0.0.0 255.255.255.255 12345678 down

Click in the **PPPoE** mode, and the page is shown as the following figure. In this page, you can configure parameters of this PPPoE PVC.



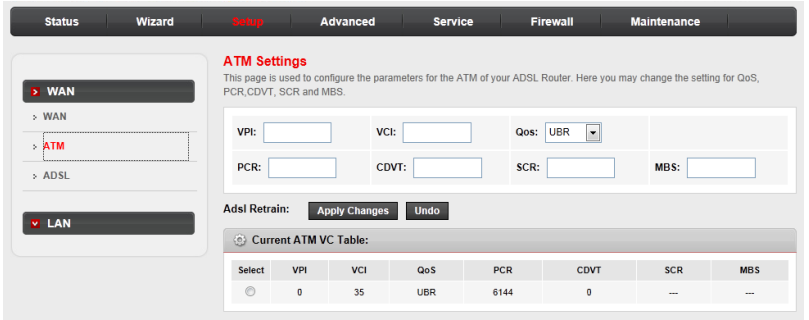
The following table describes the parameters and buttons of this page:

Field	Description
Protocol	It displays the protocol type used for this WAN

Field	Description
	connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose **AUTO**, **PAP** or **CHAP**.
Connection Type	You can choose **Continuous**, **Connect on Demand** or **Manual**.
Idle Time (s)	If choose **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
Bridge	You can select **Bridged Ethernet**, **Bridged PPPoE** or **Disable Bridge**.
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select **Disable** or **Enable**. After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
Apply Changes	Click it to save the settings of this page temporarily.
Return	Click it to return to the **Channel Configuration** page.
Reset	Click it to refresh this page.
Source Mac address	The MAC address you want to clone.
MAC Clone	Click it to enable the MAC Clone function with the MAC address that is configured.

3.4.1.2 ATM

Choose **Setup** > **WAN > ATM,** and the page is shown as the following figure. In this page you can set the parameters for the ATM, including **QoS**, **PCR**, **CDVT**, **SCR** and **MBS**.



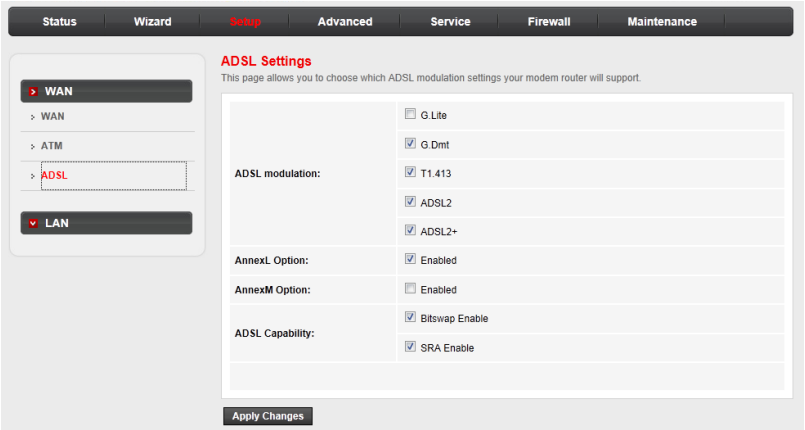
The following table describes the parameters of this page:

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose **UBR**, **CBR**, **nrt-VBR** or **rt-VBR**.
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to 4294967295.
SCR	Sustain cell rate (SCR) is the maximum rate that traffic can pass over a PVC without the risk of cell loss. Its value ranges from 0 to 65535.
MBS	Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR. Its value ranges from 0 to 65535.

3.4.1.3 ADSL

Choose **Setup** > **WAN** > **ADSL**, and the page is shown as the following figure. In this page, you can select the **ADSL modulation**. Mostly, you need to remain this

factory default settings. The router supports these modulations: **G.Lite**, **G.Dmt**, **T1.413**, **ADSL2**, **ADSL2+**, **AnnexL**, and **AnnexM**. The router negotiates the modulation modes with the DSLAM.

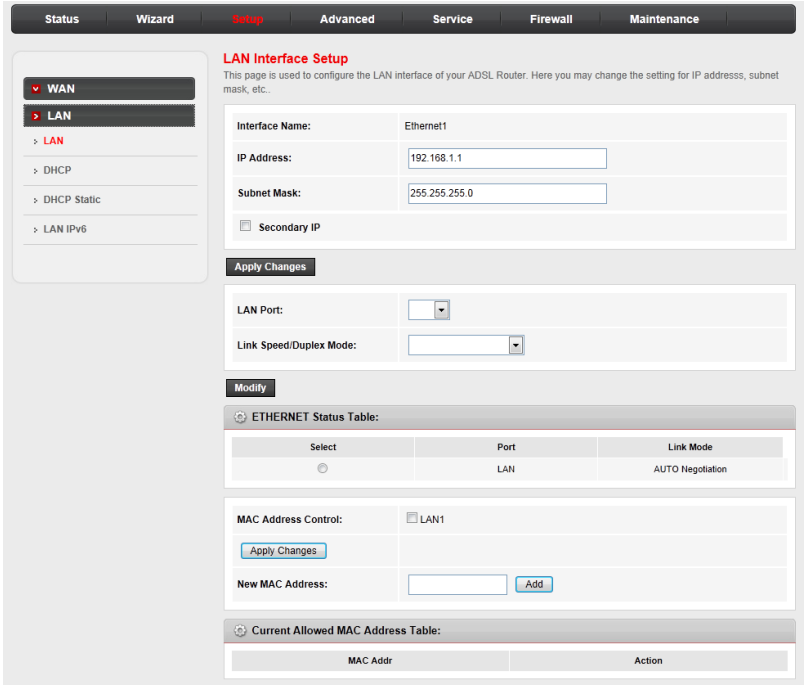


3.4.2 LAN Configuration

In the **Setup** page, click **LAN** on the left pane, and the sub-menu of the LAN includes **LAN**, **DHCP**, **DHCP Static** and **LAN IPv6**.

3.4.2.1 LAN

Choose **Setup** > **LAN,** and the page is shown as the following figure. In this page, you can change IP address and subnet mask of the router. The default IP address is **192.168.1.1**, which is the private IP address of the router.



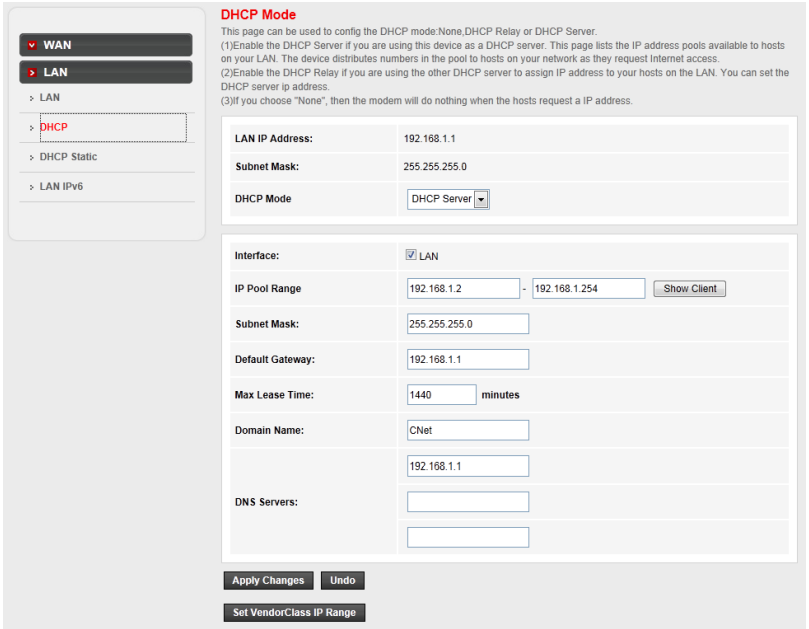
The following table describes the parameters of this page:

Field	Description
IP Address	Enter the IP address of the LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is 192.168.1.1- 192.168.255.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable a secondary LAN IP address. The two LAN IP addresses must be in the different network.
LAN Port	You can choose the LAN interface to configure.

Field	Description
Link Speed/Duplex Mode	You can select the following modes from the drop-down list: **100Mbps/FullDuplex**, **100Mbps/Half Duplex**, **10Mbps/FullDuplex**, **10Mbps/Half Duplex**, and **Auto Negotiation**.
Modify	Select the index from Ethernet Status Table, and after changing the settings, click **Modify**.
ETHERNET Status Table	It shows the current Ethernet status list. You can select the index from Ethernet Status Table to modify.
MAC Address Control	It is the access control based on MAC address. Select it and the host whose MAC address is listed in the **Current Allowed MAC Address Table** can access the modem.
New MAC Address	Enter MAC address, and then click **Add** to add a new MAC address.
Current Allowed MAC Address Table	It shows the current allowed MAC address list.

3.4.2.2 DHCP

Choose **Setup** > **LAN > DHCP**, and the page is shown as the following figure.

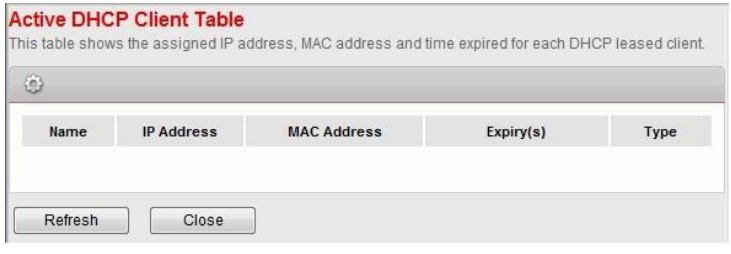

WAN
LAN
LAN
DHCP
DHCP Static
LAN IPv6
DHCP Mode
This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Mode DHCP Server
Interface: LAN
IP Pool Range 192.168.1.2 - 192.168.1.254 Show Client
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
Max Lease Time: 1440 minutes
Domain Name: CNet
DNS Servers: 192.168.1.1
Apply Changes
Undo
Set VendorClass IP Range

The following table describes the parameters of this page:

Field	Description
DHCP Mode	You can choose **None**, **DHCP Relay** and **DHCP Server**. If set to **DHCP Server**, the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows95, Windows NT and other operation systems that support the DHCP client.
IP Pool Range	It specifies the first IP address in the IP address pool. The router assigns IP address that base on the IP pool range to the host.
Show Client	Click it, the **Active DHCP Client Table** appears. It shows IP addresses assigned to clients.
Subnet Mask	Enter the subnet mask.

Field	Description
Default Gateway	Enter the default gateway of the IP address pool.
Max Lease Time	The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Domain Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
DNS Servers	You can configure the DNS server IP addresses for DNS Relay.
Set VendorClass IP Range	Click it, the **Device IP Range Table** page appears. You can configure the IP address range based on the device type.

Click **Show Client** in the **DHCP Mode** page, and the page is shown as the following figure. You can view the IP address assigned to each DHCP client.

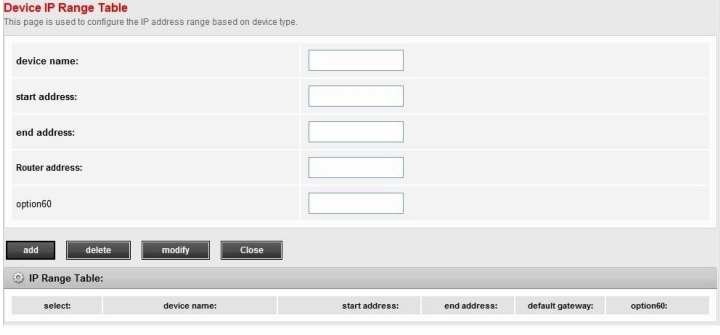


The following table describes the parameters and buttons in this page:

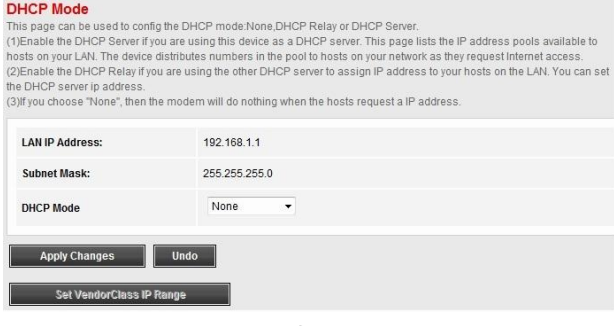
Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it

Field	Description
	consists of six pairs of hexadecimal character, for example, 00-08-A1-12-34-56.
Expiry (s)	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

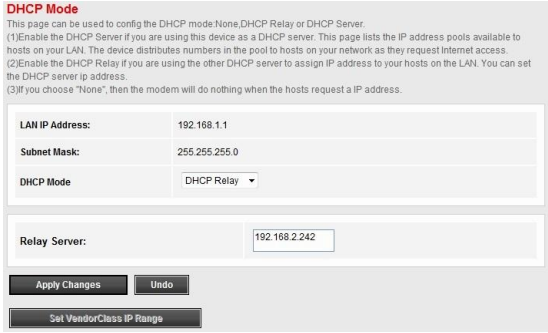
Click **Set VendorClass IP Range** in the **DHCP Mode** page, and the page is shown as the following figure. In this page, you can configure the IP address range based on the device type.



Choose **None** in the **DHCP Mode** field, and the page is shown as the following figure.


DHCP Mode
This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.
LAN IP Address:
192.168.1.1
Subnet Mask:
255.255.255.0
DHCP Mode
None
Apply Changes
Undo
Set VendorClass IP Range

In the **DHCP Mode** field, choose **DHCP Relay**. The page is shown as the following figure.

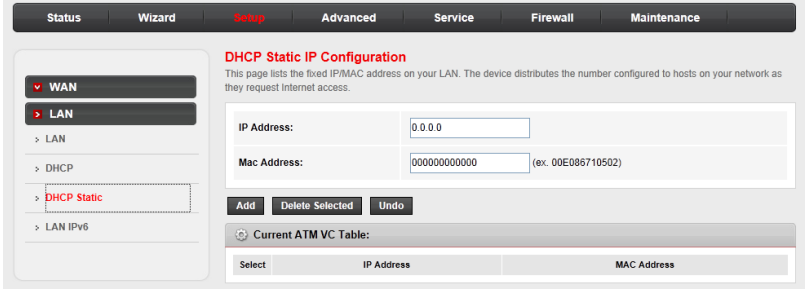

DHCP Mode
This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.
LAN IP Address:
192.168.1.1
Subnet Mask:
255.255.255.0
DHCP Mode
DHCP Relay
Relay Server:
192.168.2.242
Apply Changes
Undo
Set VendorClass IP Range

The following table describes the parameters and buttons of this page:

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings of this page.
Undo	Click it to erase the change and revert it to the last settings.

3.4.2.3 DHCP Static

Choose **Setup** > **LAN > DHCP Static,** and the page is shown as the following figure. In this page, you can assign the IP addresses to the specific individual PCs based on their MAC address.

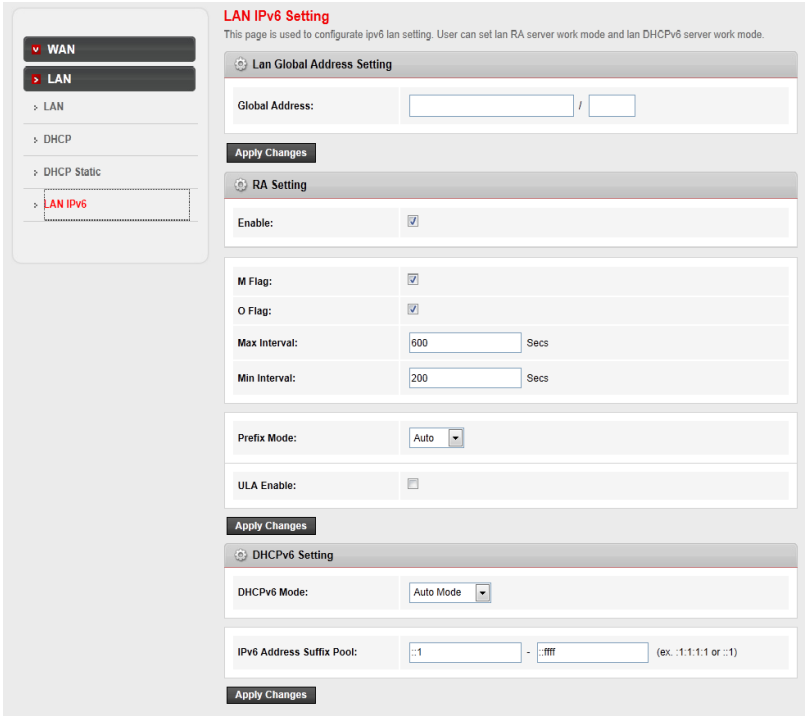


The following table describes the parameters and buttons of this page:

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
Mac Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click **Add**. An added row will be presented in the **Current ATM VC Table**.
Delete Selected	Select a row in the **Current ATM VC Table**, and then click **Delete Selected**, and this row will be deleted.
Undo	Click it to erase the change and revert it to the last settings.
Current ATM VC Table	It shows the assigned IP address based on the MAC address.

3.4.2.4 LAN IPv6

Choose **Setup** > **LAN > LAN IPv6,** and the page is shown as the following figure. In this page, you can modify the IPv6 LAN parameters including the settings of LAN RA server work mode and LAN DHCPv6 server work mode



The following table describes the parameters and buttons of this page:

Field	Description
Global Address	Specify the LAN global IPv6 address, may be assigned by ISP.
RA Setting	
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “Other configuration” flag in RA packet.

Field	Description
Max Interval	Maximum sending time interval.
Min Interval	Minimum sending time interval.
Prefix Mode	Specify the RA feature prefix mode: **Auto**: The RA prefix will use WAN dhcp-pd prefix **Manual**: User will specify the prefix Address, Length, Preferred time and Valid time.
DHCPv6 Mode	Specify the DHCPv6 server mode: **None**: Close DHCPv6 server. **Manual**: DHCPv6 server is opened and user specifies the DHCPv6 server address pool and other parameters. **Auto**: DHCPv6 server is opened and it uses WAN dhcp-pd prefix to generate address pool.

3.5 Advanced

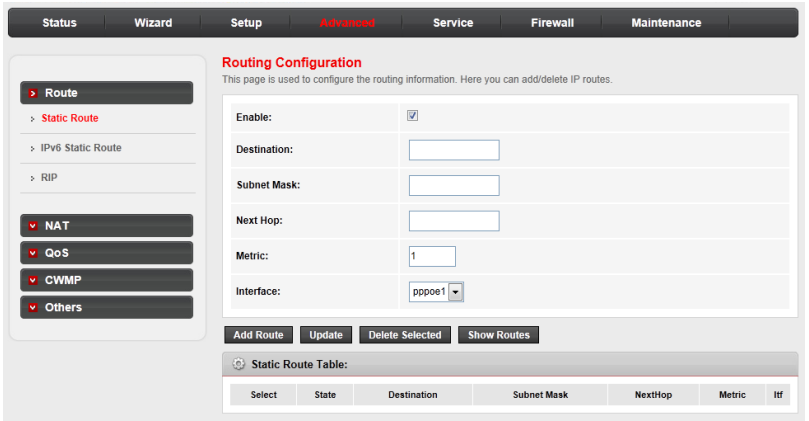
In the navigation bar, click **Advanced**. The **Advanced** contains **Route**, **NAT**, **QoS**, **CWMP** and **Others**.

3.5.1 Route

In the **Advanced** page, click **Route** on the left pane, and the sub-menu of **Route** includes **Static Route**, **IPv6 Static Route** and **RIP**.

3.5.1.1 Static Route

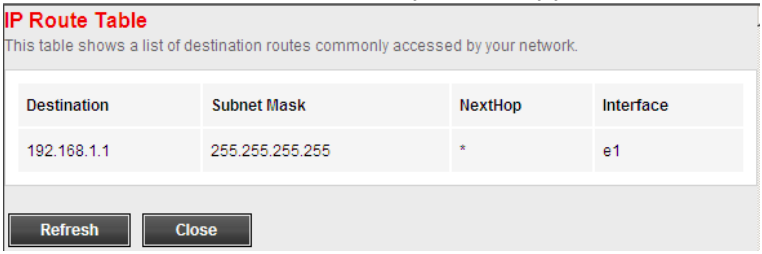
Choose **Advanced** > **Route** > **Static Route**, and the page is shown as the following figure. This page is used to configure the routing information. You can add or delete IP routes.



The following table describes the parameters and buttons of this page:

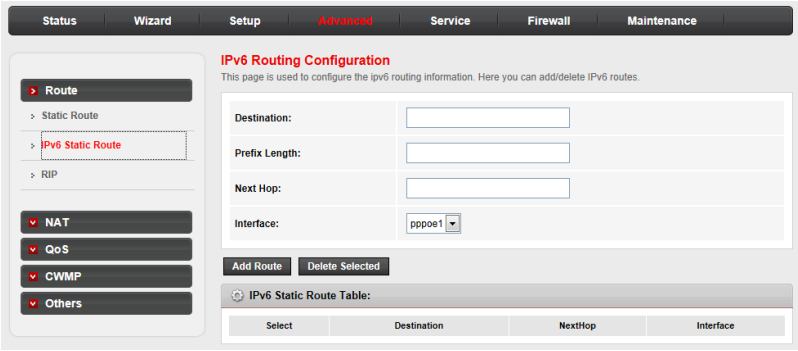
Field	Description
Enable	Select it to use static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the **Static Route Table**.
Update	Select a row in the **Static Route Table** and modify the parameters. Then click it to save the settings.
Delete Selected	Select a row in the **Static Route Table** and click it to delete the row.
Show Routes	Click it, the **IP Route Table** appears. You can view a list of destination routes commonly accessed by your network.
Static Route Table	A list of the previously configured static IP routes.

Click **Show Routes**, and the page is shown as the following figure. The table shows a list of destination routes commonly accessed by your network.



3.5.1.2 IPv6 Static Route

Choose **Advanced** > **Route** > **IPv6 Static Route**, and the page is shown as the following figure. This page is used to configure the IPv6 routing information.



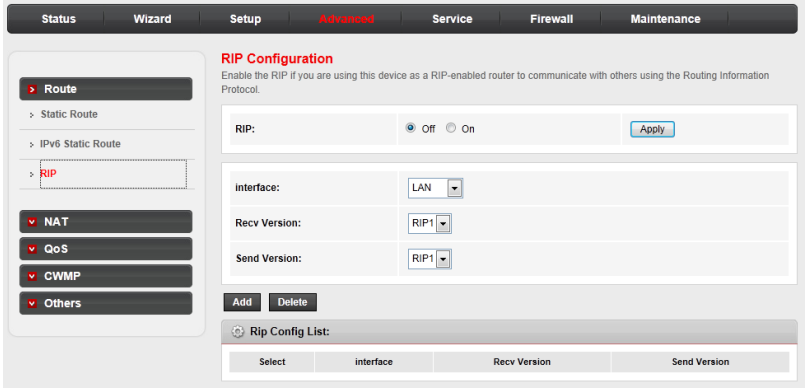
The following table describes the parameters and buttons of this page:

Field	Description
Destination	Enter the IPv6 address of the destination device.
Prefix Length	Enter the prefix length of the IPv6 address.
Next Hop	Enter the IP address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the **IPv6**

Field	Description
	Static Route Table.
Delete Selected	Select a row in the **IPv6 Static Route Table** and click it to delete the row.

3.5.1.3 RIP

Choose **Advanced** > **Route** > **RIP**, and the page is shown as the following figure. If you are using this device as a RIP-enabled router to communicate with others using Routing Information Protocol (RIP), enable RIP. This page is used to select the interfaces on your devices that use RIP, and the version of the protocol used.



The following table describes the parameters and buttons of this page:

Field	Description
RIP	Select **On**, and the router will communicate with other RIP-enabled devices.
Apply	Click it to save the settings of this page.
Interface	Choose the router interface that uses RIP.
Recv Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2** or **Both**. ● Choose **RIP1** that indicates the router receives RIP v1 messages. ● Choose **RIP2** that indicates the router receives

Field	Description
	RIP v2 messages. ● Choose **Both** that indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Choose **RIP1** that indicates the router broadcasts RIP1 messages only. ● Choose **RIP2** that indicates the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the **Rip Config List**.
Delete	Select a row in the **Rip Config List** and click it to delete the row.

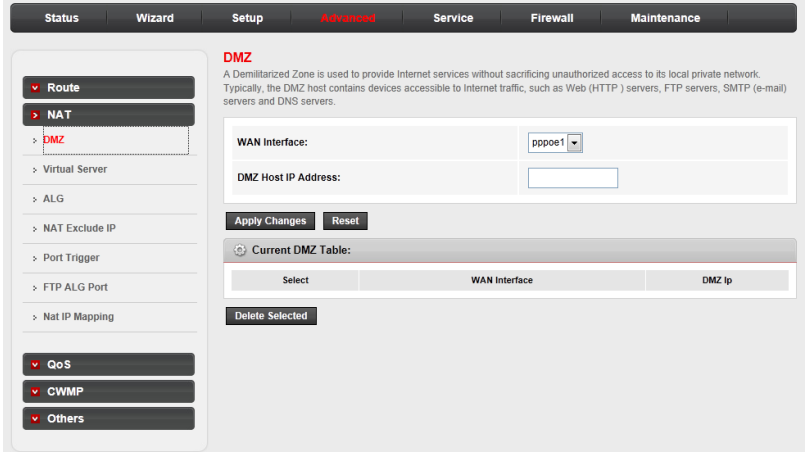
3.5.2 NAT

In the **Advanced** page, click **NAT** on the left pane, and the sub-menu of **NAT** includes **DMZ**, **Virtual Server**, **ALG**, **NAT Exclude IP**, **Port Trigger**, **FTP ALG Port** and **NAT IP Mapping**.

3.5.2.1 DMZ

Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Choose **Advanced** > **NAT** > **DMZ**, and the page is shown as the following figure.

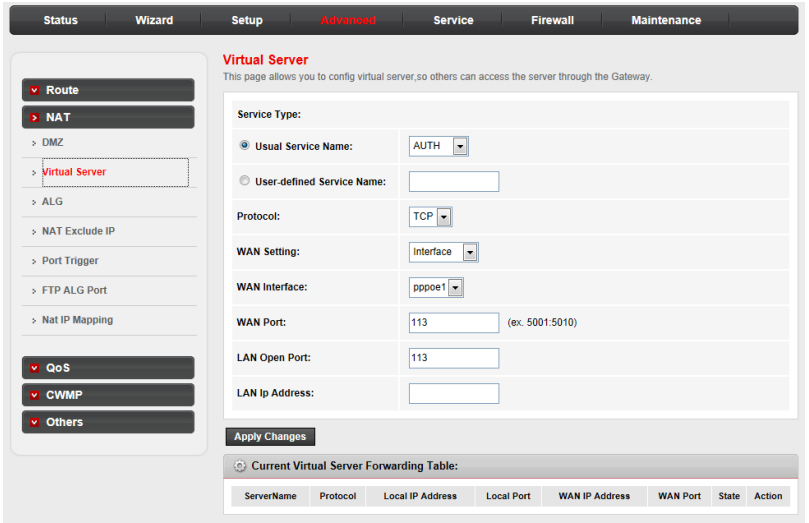


The following table describes the parameters of this page:

Field	Description
WAN Interface	Choose a WAN Interface.
DMZ Host IP Address	Enter an IP address of the DMZ host
Current DMZ Table	A list of the previously configured DMZ information

3.5.2.2 Virtual Server

Choose **Advanced** > **NAT** > **Virtual Server**, and the page is shown as the following figure. In this page you can configure virtual server, so others can access the server through the Gateway.



The following table describes the parameters of this page:

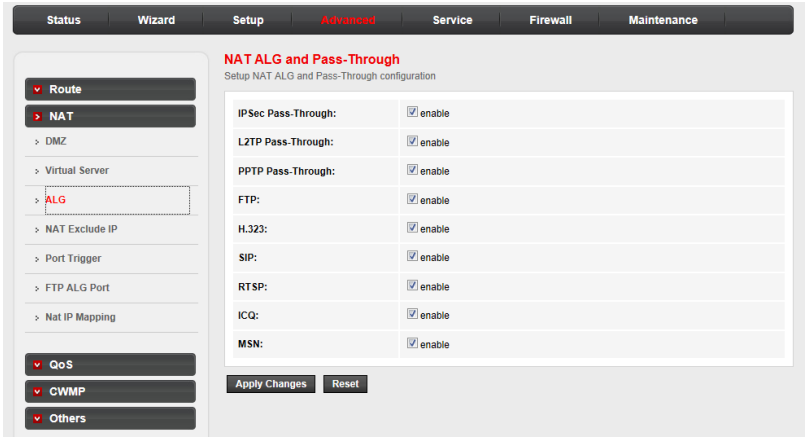
Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS**, **FTP** and so on. You can also define a service name. ● If you select **Usual Service Name**, the corresponding parameters have the default settings. ● If you select **User-defined Service Name**, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose **TCP** or **UDP**.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the WAN interface that applies to virtual server.
WAN IP Address	Enter the corresponding WAN IP Address.(Available when **IP Address** is selected in WAN Setting field.)

Field	Description
WAN Port	Choose the access port of the WAN.
LAN Open Port	Enter the port number of the specified service type.
LAN IP Address	Enter the IP address of the virtual server. It is in the same network segment with LAN IP address of the router.

3.5.2.3 ALG

The NAT ALG（Application Layer Gateways）function enables the router to support various special application protocols with payloads containing IP addresses and port numbers, and tries to establish connection between these imbedded IP addresses and port numbers. Failure of the transformation of such information may results in problems. The NAT ALG function realizes payload detection and transformation to ensure normal operation of payloads under NAT environment, requiring no special configuration of users.

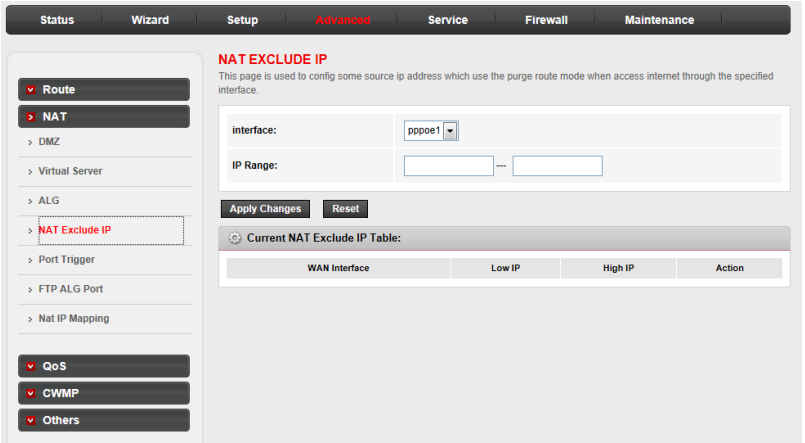
Choose **Advanced** > **NAT** > **ALG**, and the page is shown as the following figure. In this page you can set NAT ALG and pass-through configuration.



3.5.2.4 NAT Exclude IP

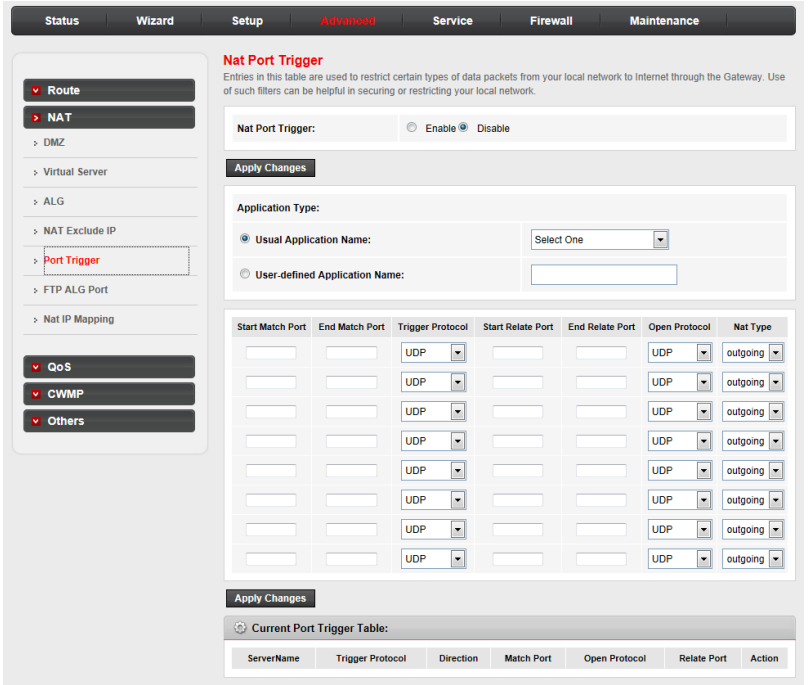
Choose **Advanced** > **NAT** > **NAT Exclude IP**, and the page is shown as the following figure. In the page, you can configure some source IP addresses which

use the purge route mode when accessing internet through the specified interface.



3.5.2.5 Port Trigger

Choose **Advanced** > **NAT** > **Port Trigger**, and the page is shown as the following figure.



Click the **Usual Application Name** drop-down menu to choose the application you want to set up for port triggering. When you have chosen an application, the default trigger settings will be generated in the table below.

If the application you want to set up is not listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port, End Match Port, Trigger Protocol, Start Relate Port, End Relate Port, Open Protocol and Nat type** settings for the port trigger you want to configure.

Click the **Apply changes** button to finish the setting.

3.5.2.6 FTP ALG Port

Choose **Advanced** > **NAT** > **FTP ALG Port**, and the page is shown as the following figure. The common port for FTP connection is port 21, and a common ALG monitors the TCP port 21 to ensure NAT pass-through of FTP. By enabling this function, when the FTPserver connection port is not a port 21, the FTP ALG module will be informed to monitor other TCP ports to ensure NAT pass-through of FTP.

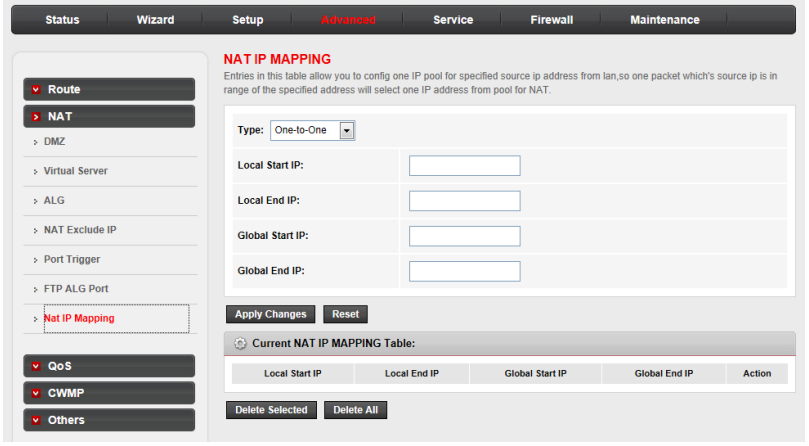
The following table describes the parameters and buttons of this page:

Field	Description
FTP ALG port	Set a FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected DestPort	Delete a selected port configuration from the list.

3.5.2.7 NAT IP Mapping

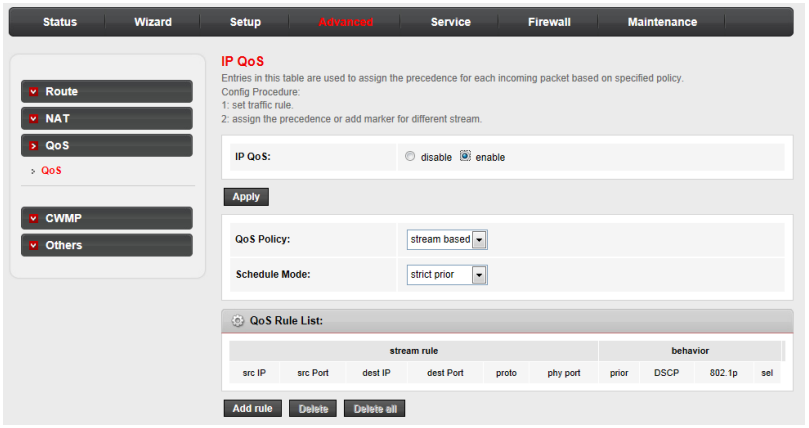
NAT is the abbreviation for Network Address Translation. The Network Address Translation Settings allow you to share one WAN IP address for multiple computers on your LAN.

Choose **Advanced** > **NAT** > **NAT IP Mapping**, and the page is shown as the following figure. This page allows you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.



3.5.3 QoS

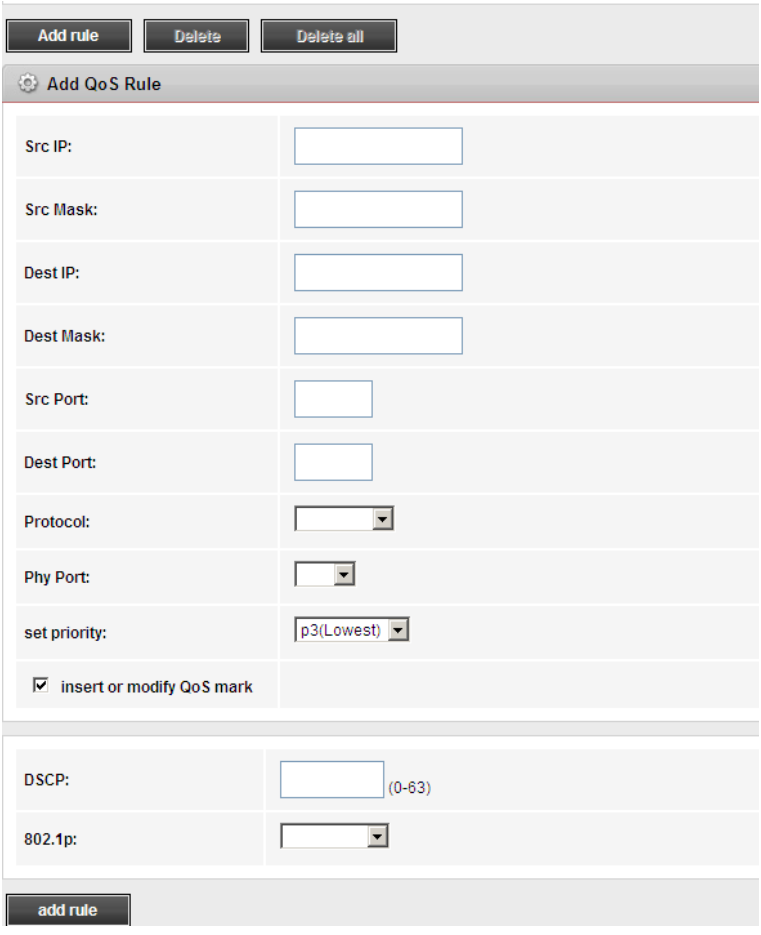
Choose **Advanced > IP QoS**, and in this page, you can enable the **IP QoS**, and the page is shown as the following figure.



The following table describes the parameters and buttons of this page:

Field	Description
IP QoS	Select to enable or disable IP QoS function. You need to enable IP QoS if you want to configure the parameters of this page.
QoS Policy	You can choose **stream based**, **802.1p based** or **DSCP based**.
Schedule Mode	You can choose **strict prior** or **WFQ (4:3:2:1)**.

Click **Add rule** at the bottom of the page and the following figure appears. Entries in the **QoS Rule List** are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, source IP address, destination IP address and other information.



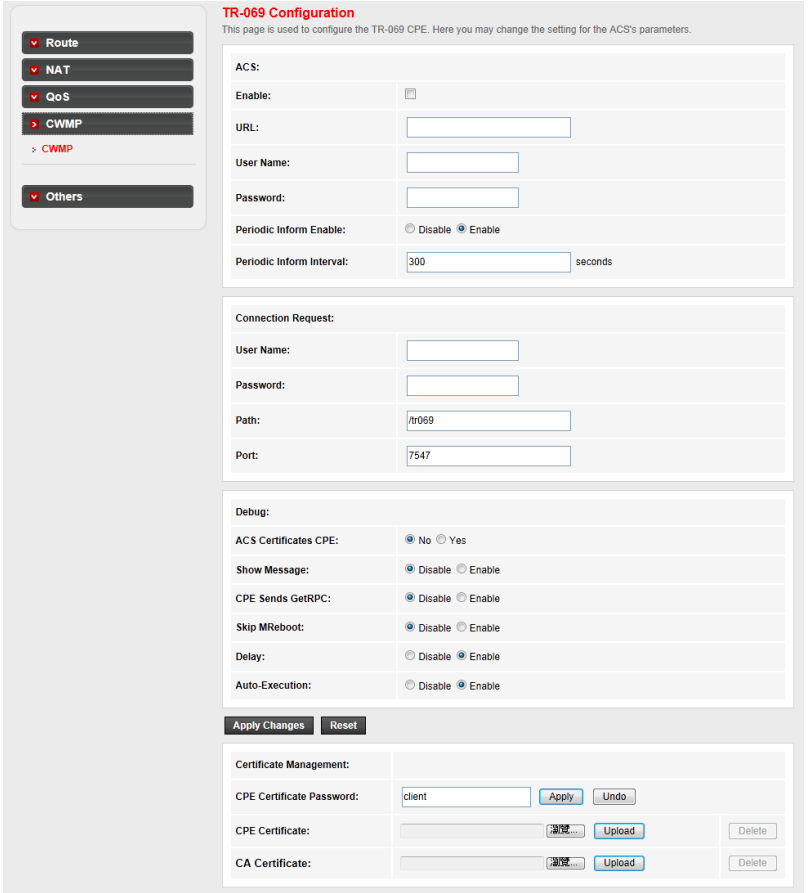
The following table describes the parameters and buttons of this page:

Field	Description
Src IP	The IP address of the source data packet.
Src Mask	The subnet mask of the source IP address.

Field	Description
Dest IP	The IP address of the destination data packet.
Dest Mask	The subnet mask of the destination IP address.
Src Port	The port of the source data packet.
Dest Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rules. You can choose **TCP**, **UDP**, or **ICMP**.
Phy Port	The LAN interface responds to the IP QoS rules.
Set priority	The priority of the IP QoS rules. P0 is the highest priority and P3 is the lowest.
Insert or modify QoS mark	Add or modify the mark (DSCP and 802.1P) of QoS
DSCP	Differentiated Services Code Point: It is one of QoS mode, and you can configure DSCP from 0 to 63.
802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization. You can choose from 0 to 7 levels.

3.5.4 CWMP

Choose **Advanced > CWMP**, and the page is shown as the following figure. In this page, you can configure the TR-069 CPE and change the setting for the ACS's parameters.



The following table describes the parameters of this page:

Field	Description
ACS	
URL	The URL of the auto-configuration server
User Name	The user name for logging in to the ACS.

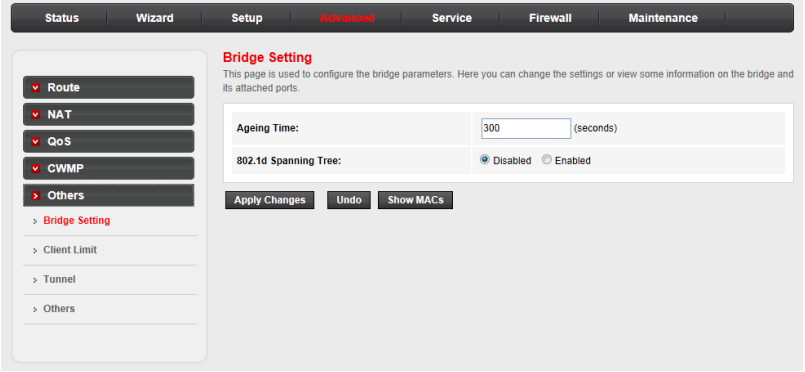
Password	The password for logging in to the ACS.
Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Path	TR-069 local path
Port	TR-069 connect port
Debug	
ACS Certificates CPE	Enable or disable the ACS Certificates
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable**, the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.
Certificate Management	
CPE Certificate Password	The Password of CPE Certificates.
CPE Cerificate	The Cerificate of CPE.
CA Certificate	The Cerificate of certificate authority.

3.5.5 Others

In the **Advanced** page, click **Others** on the left pane, and the sub-menu of **Others** includes **Bridge Setting**, **Client Limit**, **Tunnel** and **Others**.

3.5.5.1 Bridge Setting

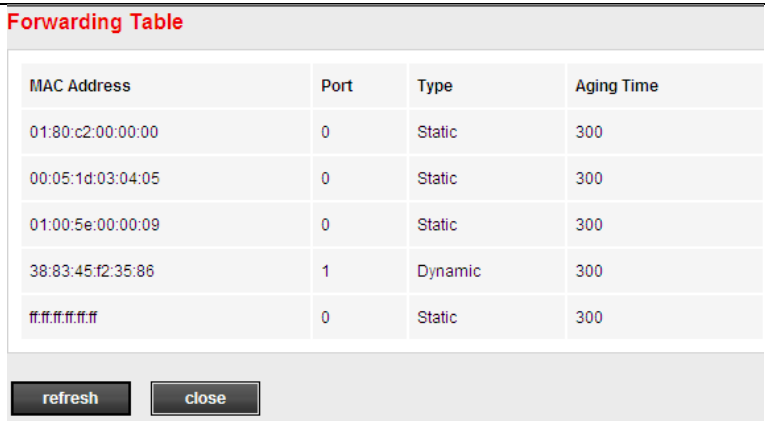
Choose **Advanced > Others > Bridge setting**, and the page is shown as the following figure. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.



The following table describes the parameters and button of this page:

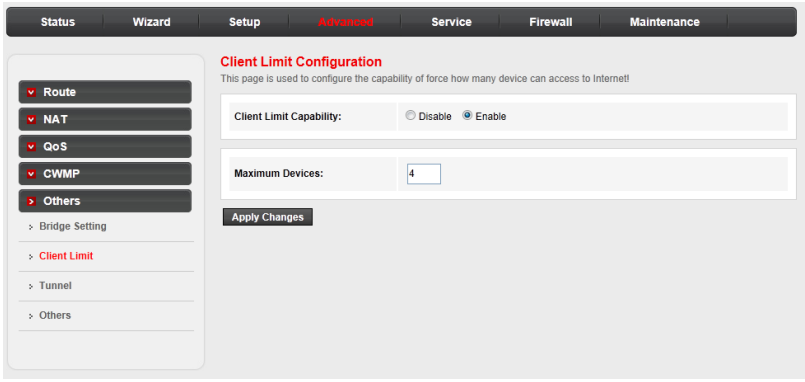
Field	Description
Aging Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
802.1d Spanning Tree	You can select **Disabled** or **Enabled**. Select **Enabled** to provide path redundancy while preventing undesirable loops in your network.
Show MACs	Click it to show a list of the learned MAC addresses for the bridge.

Click **Show MACs**, and the page is shown as the following figure. This table shows a list of learned MAC addresses for this bridge.



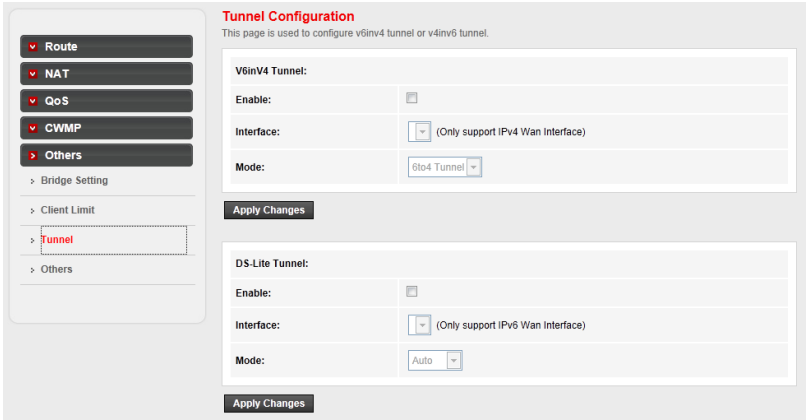
3.5.5.2 Client Limit

Choose **Advanced > Others > Client Limit**, and the page is shown as the following figure. This page is used to set the limitation on the quantity of the PCs which are allowed to connect to the router.



3.5.5.3 Tunnel

Choose **Advanced > Others > Tunnel**, and the page is shown as the following figure. This page is used to configure tunnels to connect IPv4 and IPv6 networks.

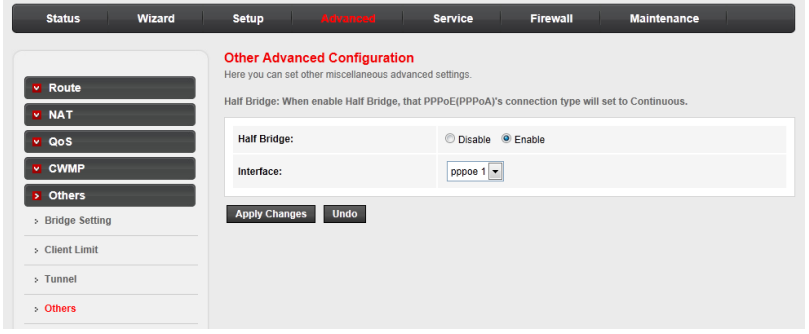


The following table describes the parameters and button of this page:

Field	Description
V6inV4 Tunnel	
Enable	Enable or Disable the V6inV4 Tunnel.
Interface Name	Select the current WAN interface used as tunnel interface.
Mode	6to4 Tunnel or 6rd Tunnel
DS-Lite Tunnel	
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select the current WAN interface used as tunnel interface.
Mode	Auto or Manual

3.5.5.4 Others

Choose **Advanced > Others > Others**, and the page is shown as the following figure. In this page, you can enable half bridge.



3.6 Service

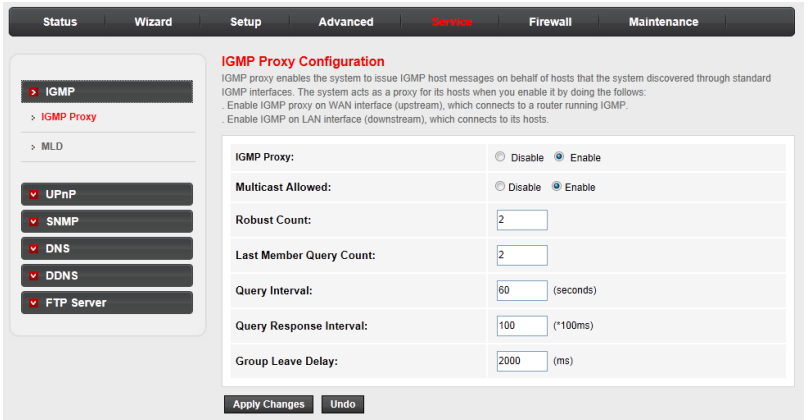
In the navigation bar, click **Service**. The **Service** page contains **IGMP**, **UPNP**, **SNMP**, **DNS**, **DDNS and FTP Server.**

3.6.1 IGMP

In the **Service** page, click **IGMP** on the left pane, and the sub-menu of **IGMP** includes **IGMP Proxy** and **MLD**.

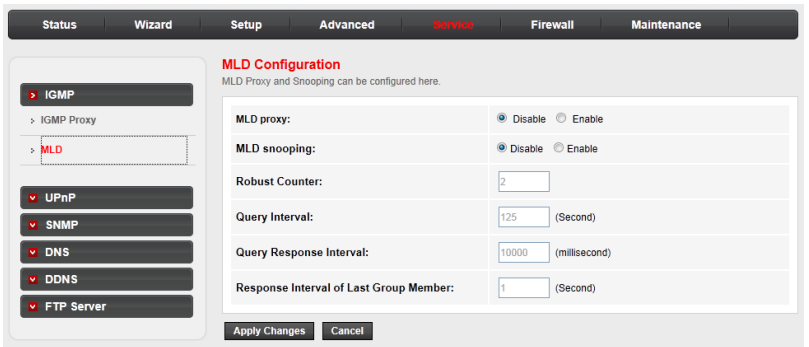
3.6.1.1 IGMP Proxy

Choose **Service** > **IGMP** > **IGMP Proxy**, and the page is shown as the following figure. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.



3.6.1.2 MLD

Choose **Service** > **IGMP** > **MLD**, and the page is shown as the following figure.



The following table describes the parameters and button of this page:

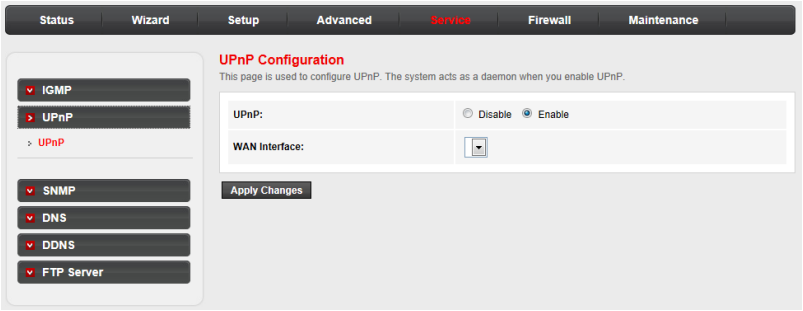
Field	Description
Enable MLD Proxy	MLD Proxy can be used to support IPv6 multicast data.
Enable MLD	Multicast Listener Discovery Snooping (MLD

Field	Description
Snooping	Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.
Robust Counter	Robust factor of the MLD Counter.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Response Interval of Last Group Member	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

3.6.2 UPnP

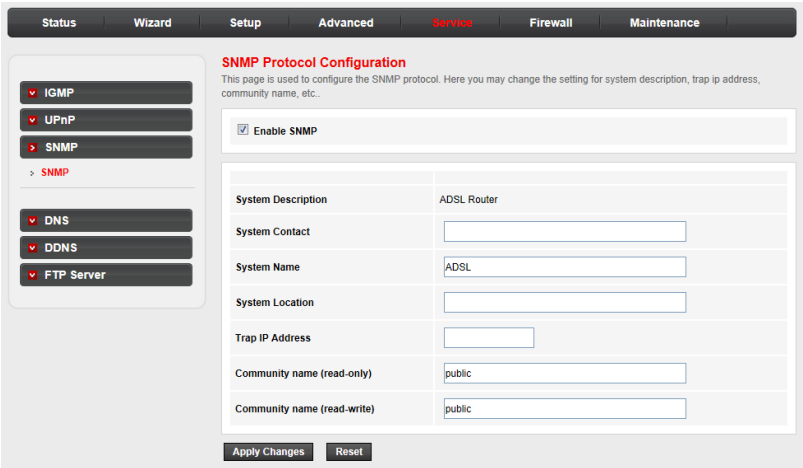
Choose **Service** > **UPnP**, and the page is shown as the following figure.

This page is used to configure UPnP. The system acts as a daemon after you enable it.



3.6.3 SNMP

Choose **Service** > SNMP, and Click **Enable SNMP**, and then the page is shown as the following figure. This page is used to configure the SNMP protocol.



The following table describes the parameters of this page:

Field	Description

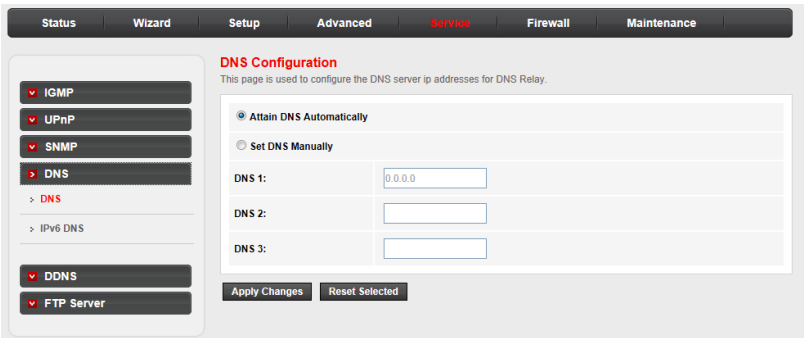
Enable SNMP	Select it to enable SNMP function. You need to enable SNMP, and then you can configure the parameters of this page.
System Contact	The contract of system
System Name	The name of system
System Location	The location of system
Trap IP Address	Enter the trap IP address. The trap information is sent to the corresponding host.
Community name (read-only)	The network administrators must use this password to read the information of this router.
Community name (read-write)	The network administrators must use this password to configure the information of the router.

3.6.4 DNS

In the **Service** page, click **DNS** on the left pane, and the sub-menu of **DNS** includes **DNS** and **IPv6 DNS**:

3.6.4.1 DNS

Choose **Service** > **DNS**, and the page is shown as the following figure. This page is used to configure the DNS server IP addresses for DNS Relay.



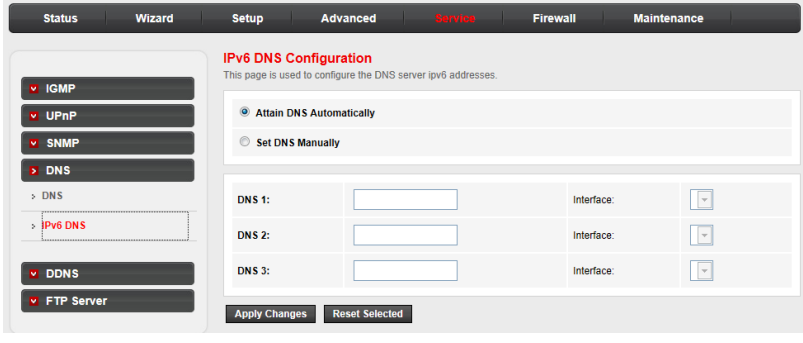
The following table describes the parameters and buttons of this page:

Field	Description

Field	Description
Attain DNS Automatically	Select it, and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it to enter the IP addresses of the primary and secondary DNS server.
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

3.6.4.2 IPv6 DNS

Choose **Service** > **DNS** > **IPv6 DNS,** and the page is shown as the following figure. This page is used to configure the DNS server IPv6 addresses.

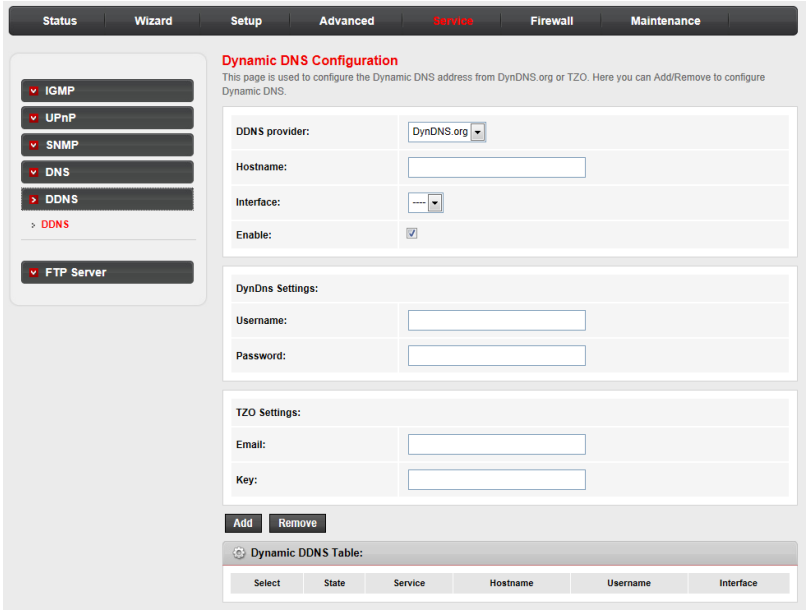


The following table describes the parameters and buttons of this page:

Field	Description
Attain DNS Automatically	Select it, the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it to enter the IP addresses and choose the WAN interface of the primary, the secondary and the tertiary DNS server.
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

3.6.5 DDNS

Choose **Service** > **DDNS**, and the page is shown as the following figure. This page is used to configure the dynamic DNS address from DynDNS.org or TZO. You can add or remove to configure dynamic DNS.



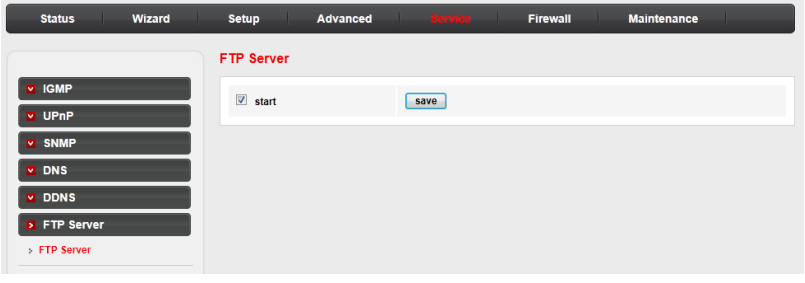
The following table describes the parameters of this page:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose **DynDNS.org**, **TZO** or **PHDNS**.
Hostname	The DDNS identifier.
Interface	The WAN interface of the router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.
Email	The email provided by DDNS provider.

Field	Description
Key	The key provided by DDNS provider.

3.6.6 FTP Server

Choose **Service** > **FTP Server**, and the page is shown as the following figure. This page is used to start the FTP Server.

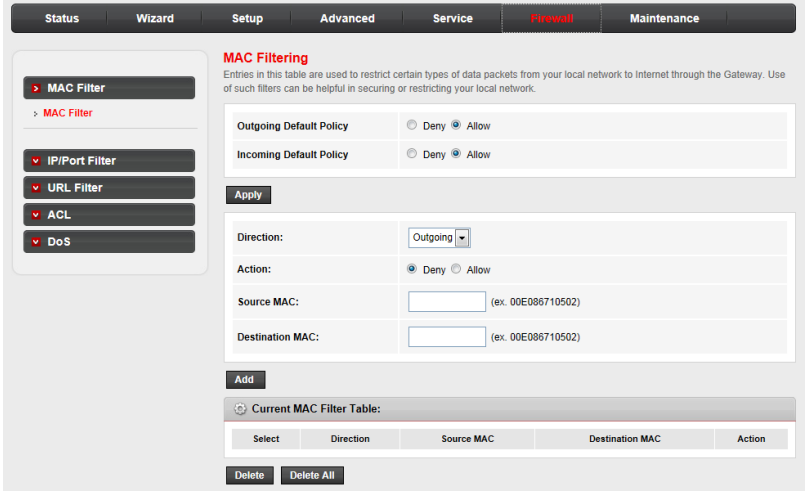


3.7 Firewall

In the navigation bar, click **Firewall**. The **Firewall** page contains **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL** and **DoS.**

3.7.1 MAC Filter

Choose **Firewall** > **MAC Filter**, and the page is shown as the following figure. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.

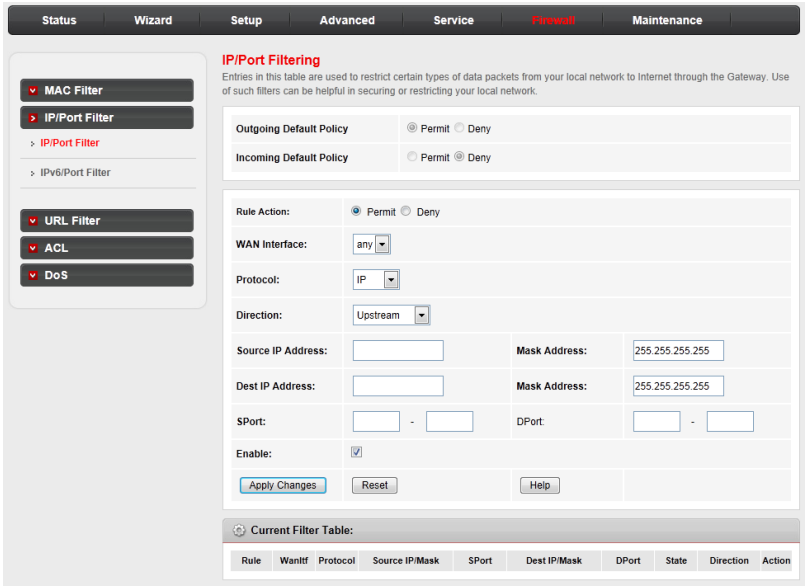


3.7.2 IP/Port Filter

In the **Firewall** page, click **IP/Port Filter** on the left pane, and the sub-menu of **IGMP** includes **IP/Port Filter** and **IPv6/Port Filter**.

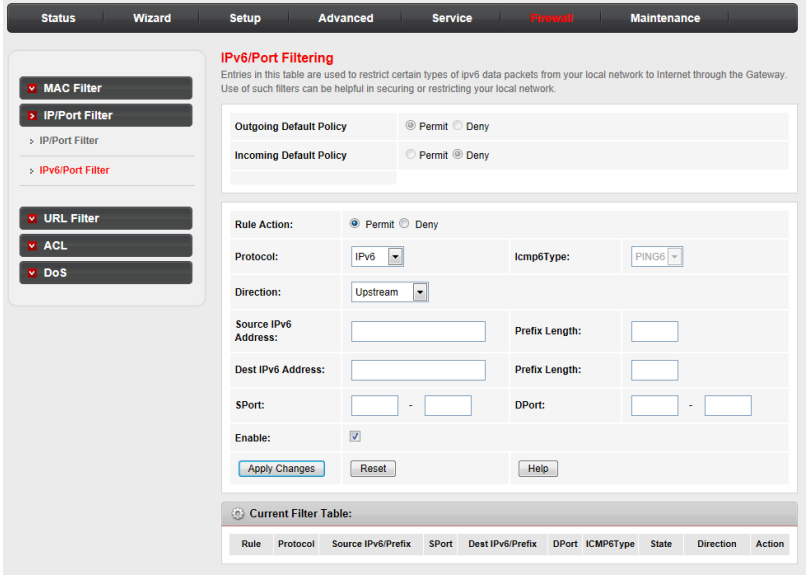
3.7.2.1 IP/Port Filter

Choose **Firewall** > **IP/Port Filter,** and the page is shown as the following figure. This part is used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



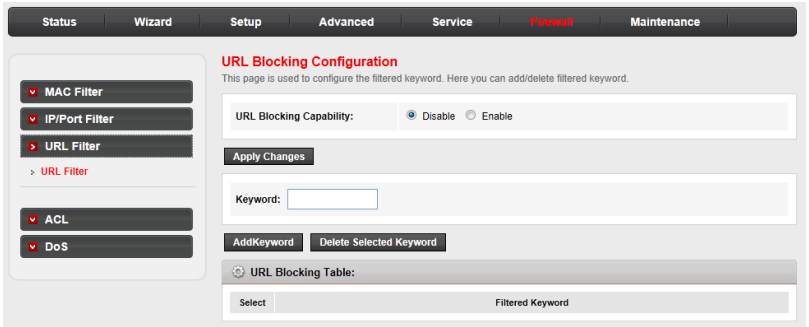
3.7.2.2 IPv6/Port Filter

Choose **Firewall** > **IP/Port Filter** > **IPv6/Port Filter,** and the page is shown as the following figure.



3.7.3 URL Filter

Choose **Firewall** > **URL Filter**, and the page is shown as the following figure. This page is used to block a fully qualified domain name, such as tw.yahoo.com and filtered keyword. You can add or delete filtered keyword.



The following table describes the parameters and buttons of this page:

Field	Description
URL Blocking Capability	You can choose **Disable** or **Enable**. ● Select **Disable** to disable URL blocking function and keyword filtering function. ● Select **Enable** to block access to the URLs and keywords specified in the **URL Blocking Table**.
Keyword	Enter the keyword to block.
AddKeyword	Click it to add a keyword to the **URL Blocking Table**.
Delete Selected Keyword	Select a row in the **URL Blocking Table** and click it to delete the row.
URL Blocking Table	A list of the URL (s) to which access is blocked.

3.7.4 ACL

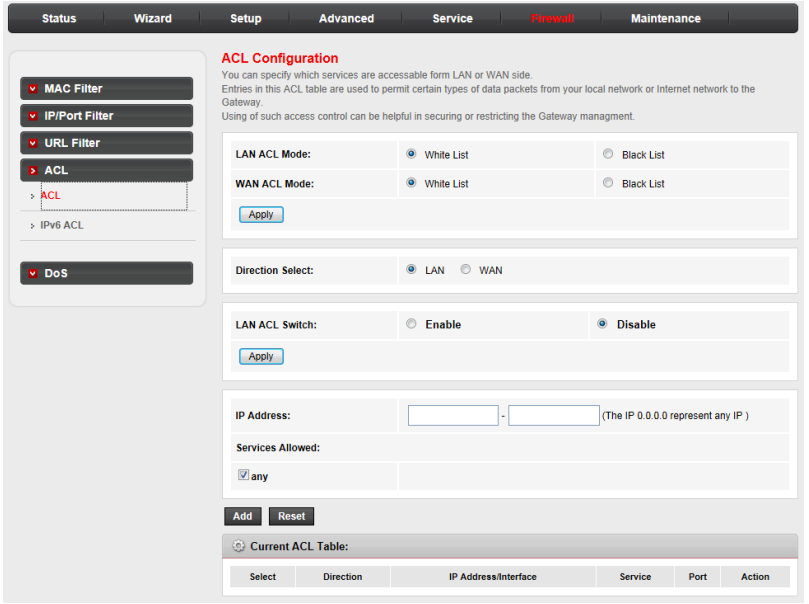
In the **Firewall** page, click **ACL** on the left pane, and the sub-menu of **ACL** includes **ACL** and **IPv6 ACL**.

Note:

If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.

3.7.4.1 ACL

Choose **Firewall** > **ACL**, and the page is shown as the following figure. In this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

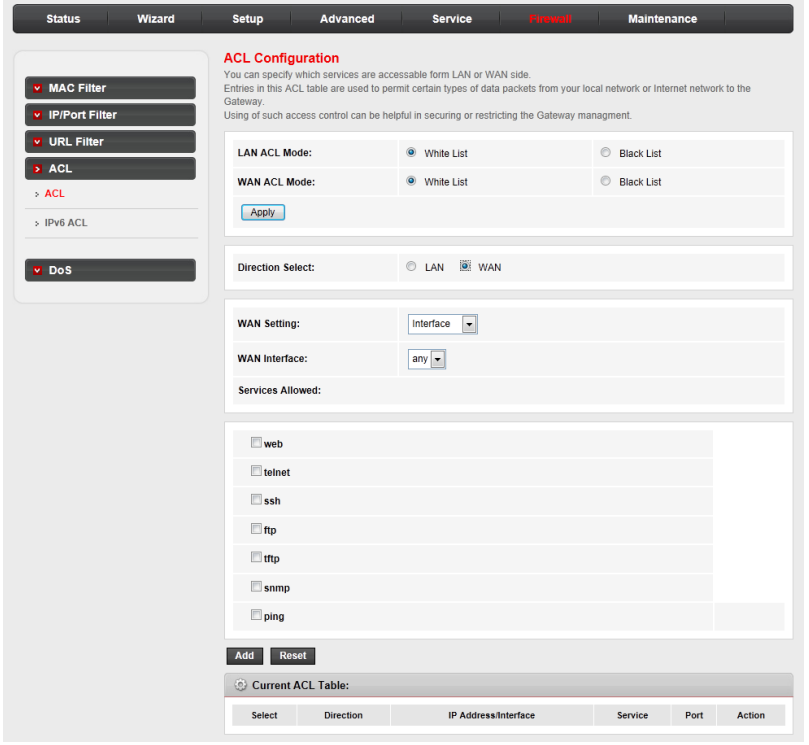


The following table describes the parameters and buttons of this page:

Field	Description
LAN ACL Mode	• When you click **White List**, only the devices whose IP addresses are listed in the **Current ACL Table** can access the router. • When you click **Black List**, the devices whose IP addresses are listed in the **Current ACL Table** are denied to access the router.
WAN ACL Mode	• When you click **White List**, only the devices whose IP addresses are listed in the **Current ACL Table** can access the router. • When you click **Black List**, the devices whose IP addresses are listed in the **Current ACL Table** are denied to access the modem.
Direction Select	Select the router interface. You can select **LAN** or

Field	Description
	WAN. In this example, **LAN** is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: **web**, **telnet**, **ssh**, **ftp**, **tftp**, **snmp** or **ping**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.
Reset	Click it to refresh this page.

If **WAN** is selected in the field of **Direction Select**, the page is shown as the following figure.



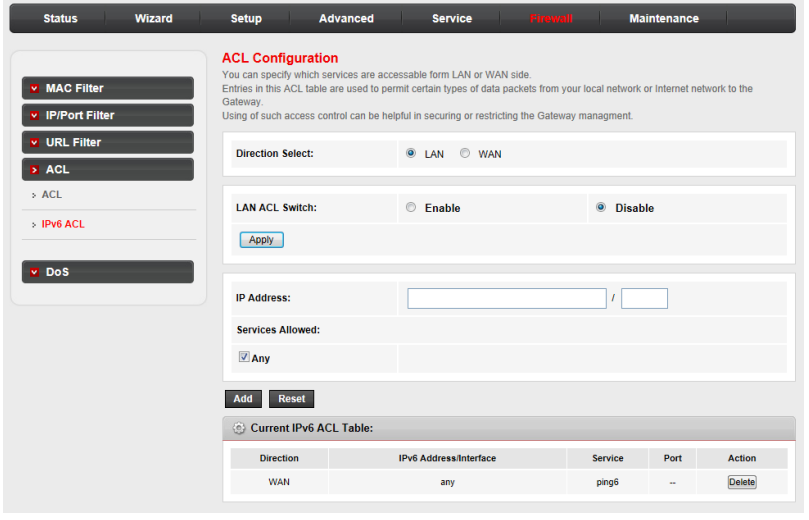
The following table describes the parameters and buttons of this page:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **WAN** is selected.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the interface that permits data packets from WAN to access the router.
IP Address	Enter the IP address on the WAN. Only the IP address that is in the same network segment with the IP address on the WAN can access the router.
Services Allowed	You can choose the following services from WAN:

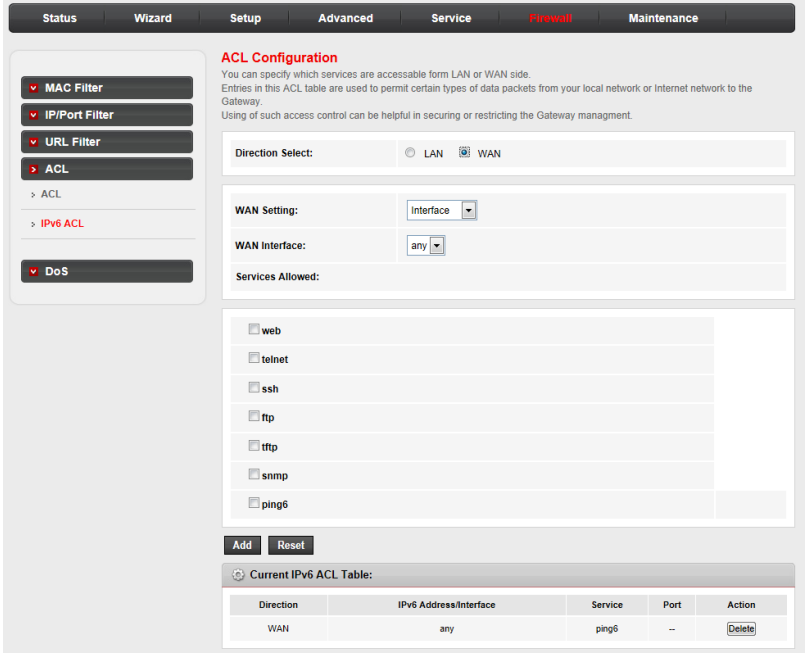
Field	Description
	web, **telnet**, **ssh**, **ftp**, **tftp**, **snmp** or **ping**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.
Reset	Click it to refresh this page.

3.7.4.2 IPv6 ACL

Choose **Firewall** > **ACL** > **IPv6 ACL**, and the page is shown as the following figure. **IPv6 ACL** has the similar function as **ACL**, and it just based on the different network protocol. For the parameters description of **IPv6 ACL**, you can refer to the **ACL**.

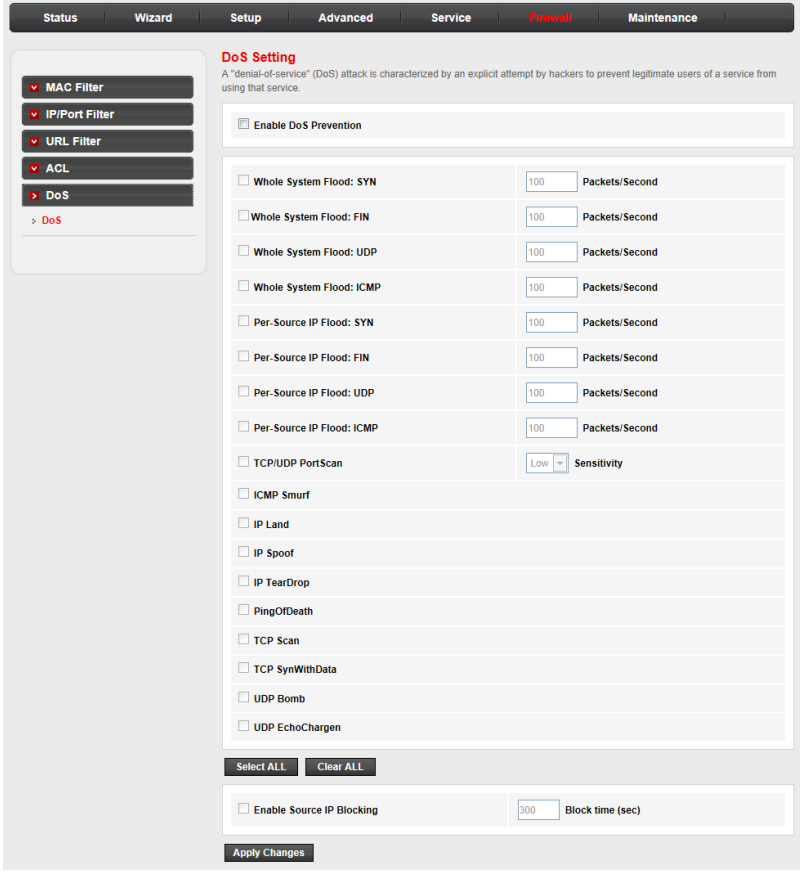


If **WAN** is selected in the field of **Direction Select**, the page is shown as the following figure.



3.7.5 DoS

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Choose **Firewall** > **DoS**, and the page is shown as the following figure. In this page, you can prevent DoS attacks.



3.8 Maintenance

In the navigation bar, click **Maintenance**. The **Maintenance** page contains **Update**, **Password**, **Reboot**, **Time, Log** and **Diagnostics**.

3.8.1 Update

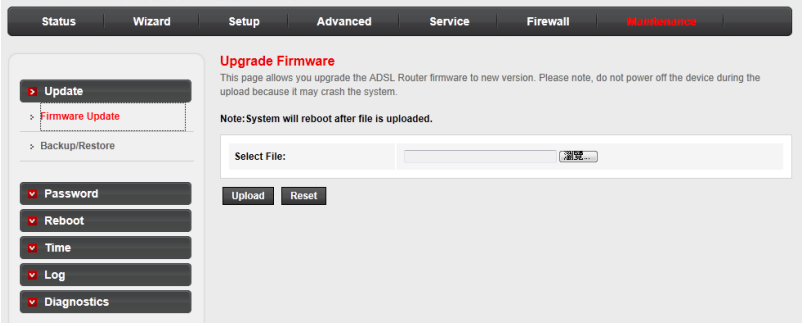
In the **Maintenance** page, click **Update** on the left pane, and the sub-menu of **Update** includes **Firmware Update** and **Backup/Restore**.

Caution:

Do not turn off the router or press the Reset button while the procedure is in progress.

3.8.1.1 Upgrade Firmware

Choose **Maintenance** > **Update**, and the page is shown as the following figure. In this page, you can upgrade the firmware of the router.

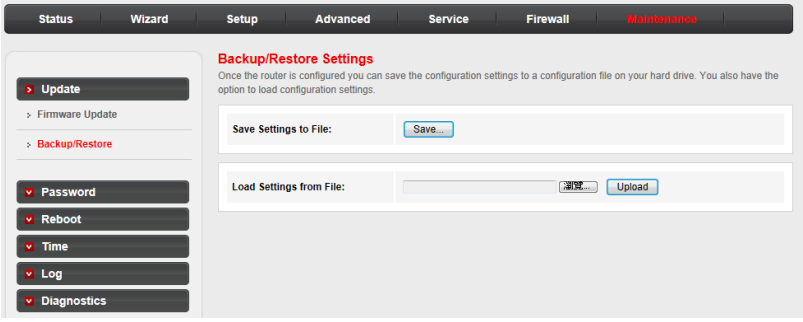


The following table describes the parameters and button of this page:

Field	Description
Select File	Click **Browse** to select the firmware file.
Upload	After selecting the firmware file, click **Upload** to upgrade the firmware file.
Reset	Click it to reselect the firmware file.

3.8.1.2 Backup/Restore

Choose **Maintenance** > **Backup/Restore**, and the page is shown as the following figure. You can backup the current settings to a file and restore the settings from the file that was saved previously.

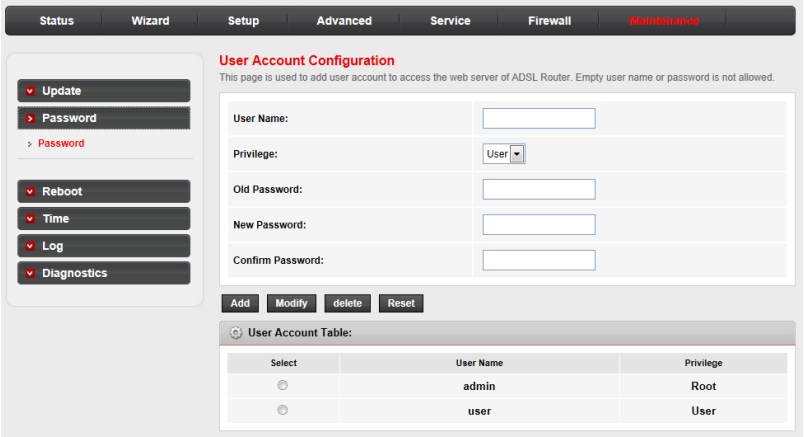


The following table describes the parameters and button of this page:

Field	Description
Save Settings to File	Click **Save** and select the path. You can save the configuration file of the router.
Load Settings from File	Click **Browse** to select the configuration file.
Upload	After selecting the configuration file of the router, click **Upload** to upload the configuration file.

3.8.2 Password

Choose **Maintenance** > **Password**, and the page is shown as the following figure. By default, the user name and password of Root are **admin** and **admin** and the user name and password of User are **user** and **user**.

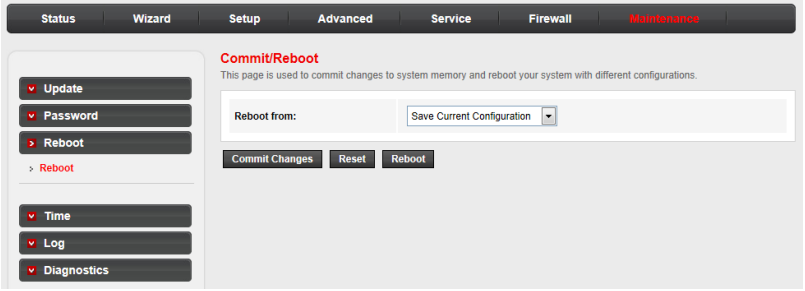


The following table describes the parameters of this page:

Field	Description
User Name	Choose the user name for accessing the router. You can choose **admin** or **user**.
Privilege	Choose the privilege for the account. You can choose **User** or **Root.**
Old Password	Enter the old password.
New Password	Enter the new password.
Confirm Password	Enter the new password again.

3.8.3 Reboot

Choose **Maintenance** > **Reboot**, and the page is shown as the following figure. You can let the router to reset to the default settings or make the router to commit the current settings.

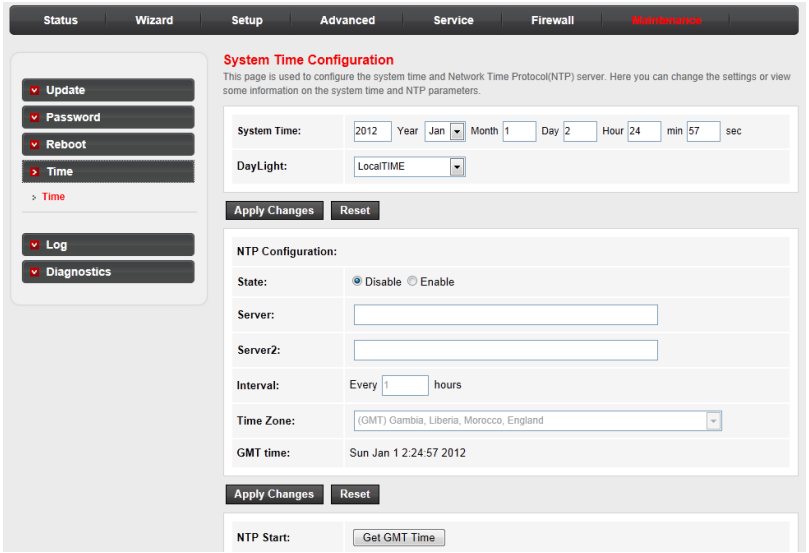


The following table describes the parameters and button of this page:

Field	Description
Reboot from	You can choose **Save Current Configuration** or **Factory Default Configuration**. ● **Save Current Configuration**: Save the current settings, and then reboot the router. ● **Factory Default Configuration**: Reset to the factory default settings, and then reboot the router.
Reboot	Click it to reboot the router.

3.8.4 Time

Choose **Maintenance** > **Time**, and the page is shown as the following figure. You can configure the system time manually or get the system time from the time server.

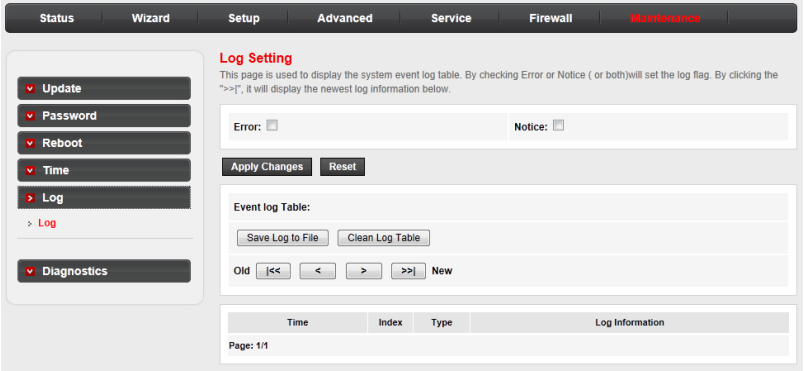


The following table describes the parameters of this page:

Field	Description
System Time	Configure the system time manually.
DayLight	Daylight Saving Time.
NTP Configuration	
State	Select enable or disable NTP function. You need to enable NTP, if you want to configure the parameters of NTP.
Server	Configure the primary NTP server manually.
Server2	Configure the secondary NTP server manually.
Interval	NTP updating time interval.
Time Zone	Choose the time zone in which area you are from the drop down list.

3.8.5 Log

Choose **Maintenance** > **Log**, and the page is shown as the following figure. In this page, you can enable or disable system log function and view the system log.

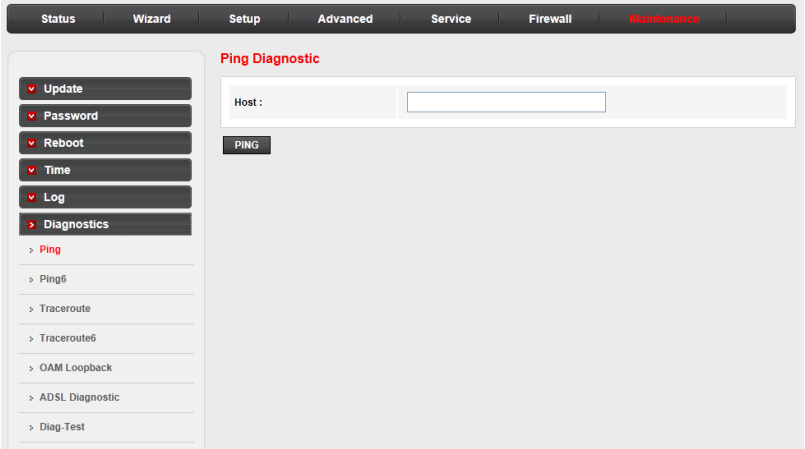


3.8.6 Diagnostics

In the **Maintenance** page, click **Diagnostics** on the left pane, and the sub-menu of **Diagnostics** includes **Ping**, **Ping6**, **Traceroute**, **Traceroute6**, **OAM Loopback**, **ADSL Diagnostic** and **Diag-Test**.

3.8.6.1 Ping

Choose **Maintenance > Diagnostics** > **Ping**, and the page is shown as the following figure.

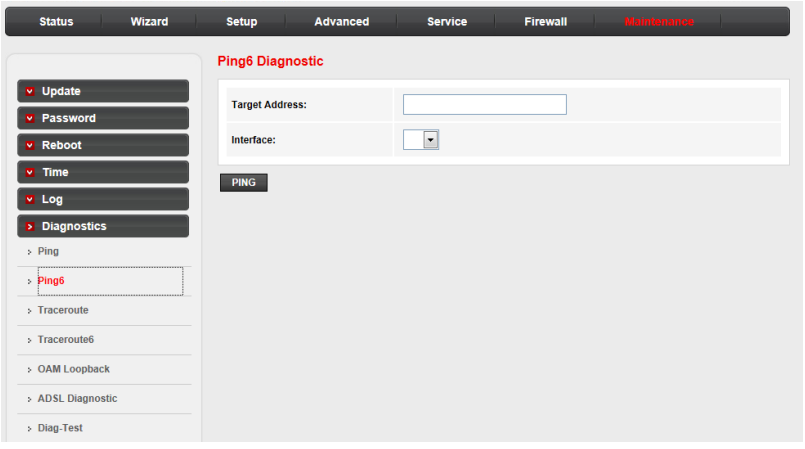


The following table describes the parameter and button of this page:

Field	Description
Host	Enter the valid IP address or domain name.
PING	Click it to start to ping.

3.8.6.2 Ping6

Choose **Maintenance > Diagnostics** > **Ping6**. The page is shown as the following figure appears.

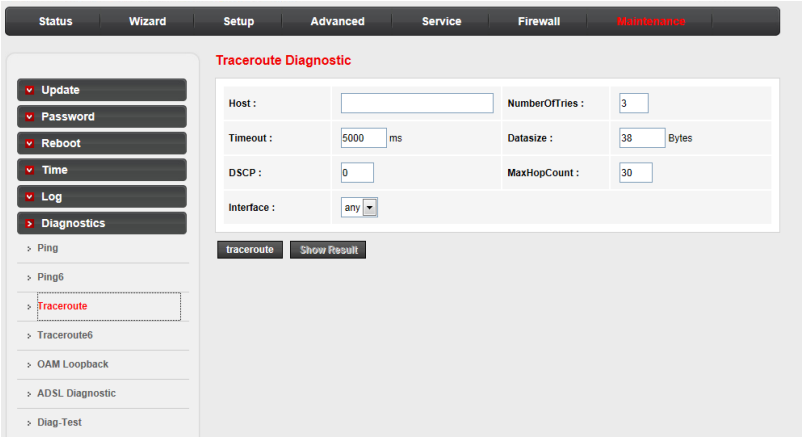


The following table describes the parameter and button of this page:

Field	Description
Target Address	Enter the valid IP address or domain name.
Interface	Choose a WAN interface.
PING	Click it to start to ping.

3.8.6.3 Traceroute

Choose **Maintenance > Diagnostics** > **Traceroute**, and the page is shown as the following figure.

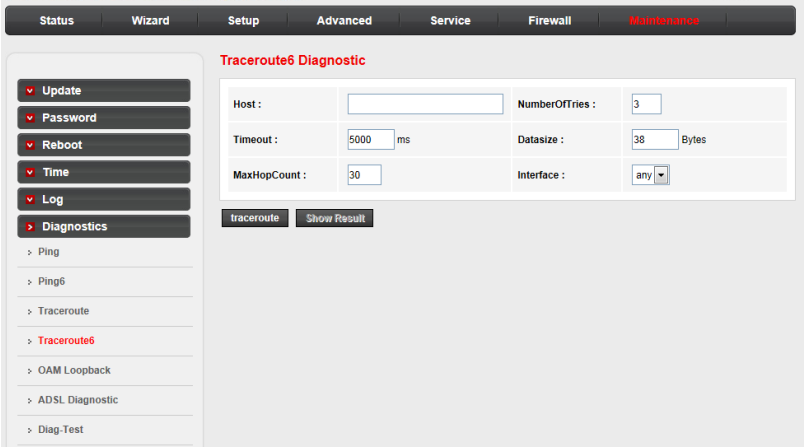


The following table describes the parameter and button of this page:

Field	Description
Host	The address of a destination host to be diagnosed.
NumberOfTries	Repeat times.
Timeout	Timeout duration.
Datasize	Data packet size.
DSCP	A differentiated services code point in the TOS identification byte for service categories in the IP header of every data packet. A DSCP prioritizes by coding values using the used 6-bit bytes and unused 2-bit bytes.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.
Traceroute	Click it to trace the route.
Show Result	Click it to display the result.

3.8.6.4 Traceroute6

Choose **Maintenance > Diagnostics** > **Traceroute6**, and the page is shown as the following figure.

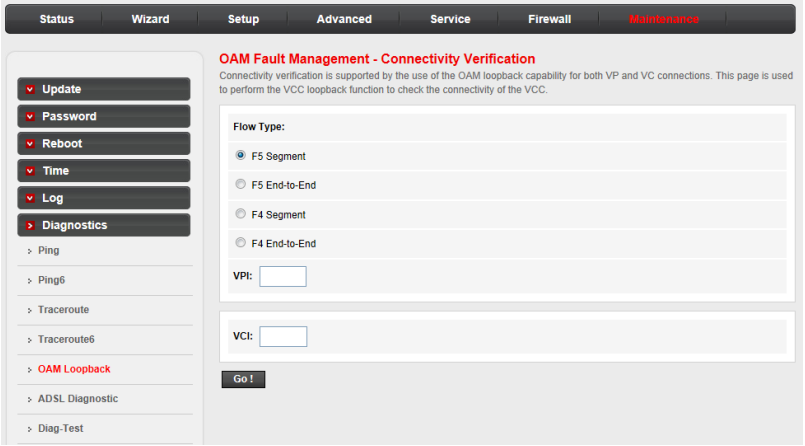


The following table describes the parameter and button of this page:

Field	Description
Host	The address of a destination host to be diagnosed.
NumberOfTries	Repeat times.
Timeout	Timeout duration.
Datasize	Data packet size.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.
Traceroute	Click it to trace the route.
Show Result	Click it to display the result.

3.8.6.5 OAM Loopback

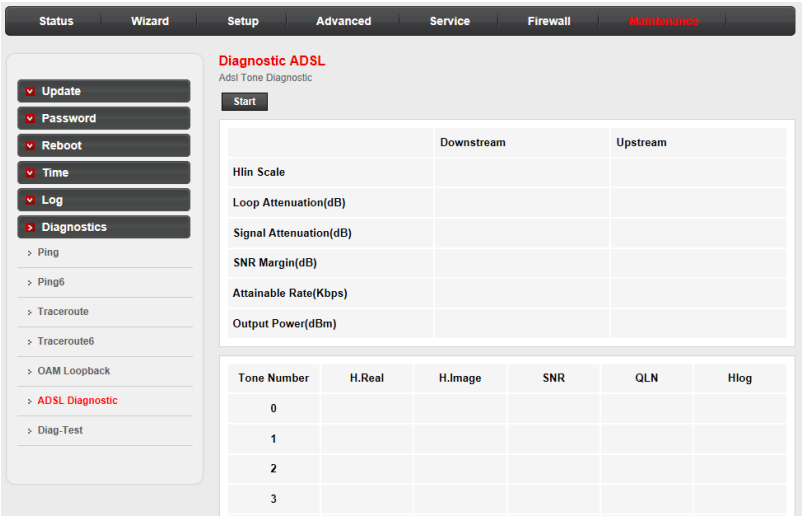
Choose **Maintenance > Diagnostics** > **OAM Loopback**, and the page is shown as the following figure. Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.



Click **GO!** to start testing.

3.8.6.6 ADSL Statistics

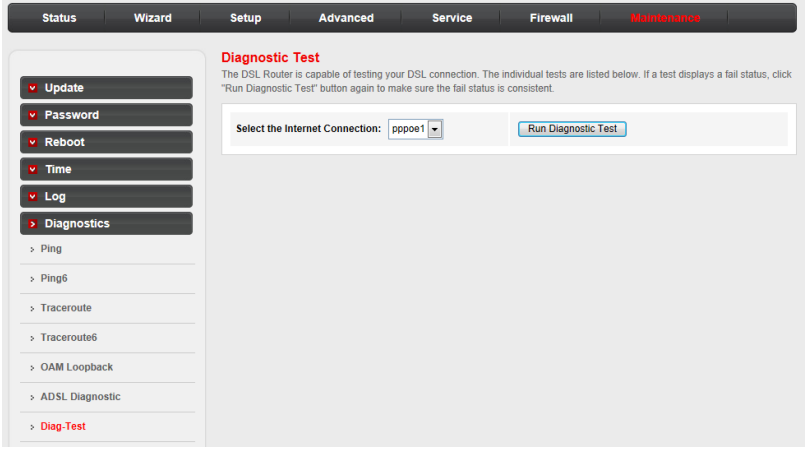
Choose **Maintenance > Diagnostics** > **ADSL Statistics**, and the page is shown as the following figure. It is used for ADSL tone diagnostics.



Click **Start** to start ADSL tone diagnostics.

3.8.6.7 Diag-Test

Choose **Maintenance > Diagnostics** > **Diag-Test**, and the page is shown as the following figure. You can test the DSL connection.



Click **Run Diagnostic Test** to start testing.

4 Troubleshooting

Question	Answer
Why are all indicates off?	• Check the connection between the power adapter and the power socket. • Check whether the power switch is turned on.
Why is the **LAN** indicator off?	Check the following: • The connection between the device and your PC, hub or switch. • The running status of the computer, hub, or switch.
Why is the **DSL** indicator off?	Check the connection between the **Line** port of the device and the wall jack.
Why Internet access fails, while the DSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why I fail to access the web configuration page of the DSL router?	Choose **Start** > **Run** from the desktop, and ping ***192.168.1.1*** (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.
How to load the default settings after incorrect configuration?	To restore the factory default settings, turn on the device, and press the reset button for about 5 seconds, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.1.1** and **255.255.255.0**, respectively. • User/password of super user: **admin/admin** • User/password of common user: **user/user**